PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-196585

(43)Date of publication of application : 14.07.2000

---

(51)Int.Cl. H04L 9/14

G11B 19/02

G11B 19/04

G11B 20/10

---

(21)Application number : 11-287365 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 07.10.1999 (72)Inventor : TAGAWA KENJI

MINAMI MASANAO

KOZUKA MASAYUKI

AOYAMA SHOICHI

TOKUDA KATSUMI

HIRATA NOBORU

---

(30)Priority

Priority number : 10286177

10297159

10297142

Priority date : 08.10.1998

19.10.1998

19.10.1998

Priority country : JP

JP

JP

---

(54) RECORDING MEDIUM RECORDING CONTENTS, DIGITAL DATA RECORDER, DIGITAL DATA REPRODUCER, CONTENTS PACKAGING DEVICE GENERATING PACKAGE, CONTENTS REPRODUCER, COMPUTER READABLE RECORDING MEDIUM, RECORDING METHOD, REPRODUCING METHOD, PACKAGING METHOD AND SYSTEM TRANSPORT STREAM PROCESSOR CONSISTING OF CONTENTS PACKAGING DEVICE AND CONTENTS REPRODUCER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a recording medium by which, to a consumer having purchased music contents, music contents relating to the music contents one sold at low cost and readily even when an infrastructure to realize electronic music distribution is not arranged.

SOLUTION: A recording medium records contents of purpose of sale and also records super distribution contents 10 that are encrypted on the basis of the block encryption method. A super distribution header 9 given to the super distribution contents 10 is encrypted on the basis of the encryption method that is an application of a public key and includes a decoding key 13 to decode the

encryption of the block encryption method. In the case that the recording medium is loaded to a device connected to a communication channel, the encryption method that is an application of the public key can be decoded by the device and the decoding of the encryption is attended with charging through the communication channel.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The 1st contents and the 2nd contents which the 1st contents are different contents and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make the encryption in the 2nd contents cancel is included. The record medium characterized by recording the header enciphered with the 2nd cipher system which is a cipher system with which discharge of the encryption is performed only when the 2nd key information beforehand distributed to predetermined equipment is used.

[Claim 2] A ****** [that said predetermined equipment has the function to charge and said header permits playback of the 2nd contents, or record to other record

media further], The use limit information which shows the count of an upper limit in the case of permitting playback or record to other record media, The record medium according to claim 1 characterized by including the accounting information which shows the tariff which record to the tariff or other record media which the playback which should be made to charge said predetermined equipment takes takes when record is permitted by playback or other record media of the 2nd contents.

[Claim 3] A ****** [that said predetermined equipment has the function to charge and said header permits playback of the 2nd contents, or record to other record media further], The authorization period information which shows the authorization period in the case of permitting record in playback or other record media, The record medium according to claim 1 characterized by including the accounting information which shows the tariff which record to the tariff or other record media which the playback which should be made to charge said predetermined equipment takes takes when record is permitted by playback or other record media of the 2nd contents.

[Claim 4] Said 1st contents are record media according to claim 1 characterized by being enciphered using the identification information of a record-medium proper.

[Claim 5] A storing means to be the digital data recording device which records

the digital data containing contents on a record medium, and to store at least one or more contents which should be recorded on a record medium, A selection means to choose the contents as superdistribution contents when what should charge record to the playback or other record media exists in said one or more contents, So that the playback about selected superdistribution contents or record to other record media may be prevented, while accounting is not performed A 1st encryption means to encipher superdistribution contents based on the 1st cipher system, A generation means to generate a superdistribution header including the key information of which encryption of superdistribution contents is made to cancel, The generated superdistribution header is enciphered based on the 2nd cipher system with safety higher than said 1st cipher system. The digital data recording device characterized by having a 2nd encryption means to give superdistribution contents, and a record means to record on a record medium by using one or more contents as digital data if a superdistribution header is given.

[Claim 6] Said digital data recording device is a digital data recording device according to claim 5 characterized by having the fetch means which takes out the identification information of a record-medium proper from a record medium further, and a 3rd encryption means to encipher about contents other than superdistribution contents using the identification information taken out by the

fetch means.

[Claim 7] The superdistribution contents which are the contents enciphered in order to prevent what recorded on other record media while accounting is required for record to other record media and accounting is not performed are read from the 1st record medium. If it is the digital data recording device recorded on the 2nd record medium and the record medium with which the charger stage loaded with either [at least] the 1st record medium or the 2nd record medium and the charger stage were loaded is the 1st record medium The read-out means which reads superdistribution contents from the 1st record medium, and a presentation means to show an operator the countervalue to record to the 2nd record medium of superdistribution contents, A discharge means to cancel encryption of the superdistribution contents read from the 1st record medium when the actuation which a reception means to receive the actuation from an operator, and the reception means received is actuation of the purport of a countervalue on which it agrees for paying, If the accounting means charged to an operator and a charger stage are loaded with the 2nd record medium used as the archive destination of superdistribution contents when directions of the purport of a countervalue on which it agrees for paying are received from an operator The digital data recording device characterized by having a record means to record on the 2nd record medium of an archive

destination by using as digital data the superdistribution contents of which encryption was canceled.

[Claim 8] If a charger stage is further loaded with the 2nd record medium used as the archive destination of superdistribution contents, said digital data recording device The fetch means which takes out the identification information of a record-medium proper from the 2nd record medium used as an archive destination, It has a re-encryption means to encipher again, using the identification information from which the fetch means took out the superdistribution contents of which encryption was canceled by the discharge means as a cryptographic key. Said record means The digital data recording device according to claim 7 characterized by recording the superdistribution contents again enciphered by the re-encryption means on the 2nd record medium of an archive destination.

[Claim 9] The charger stage which is the digital data regenerative apparatus which reproduces the superdistribution contents which are the contents enciphered in order to prevent playback while accounting is required for the playback and accounting is not performed, and loads with a record medium, The read-out means which will read this if superdistribution contents are recorded on the record medium with which the charger stage was loaded, A presentation means to show an operator the countervalue to playback of superdistribution

contents, A reception means to receive the actuation from an operator, and a discharge means to cancel encryption of superdistribution contents when the actuation which the reception means received is actuation of the purport of a countervalue on which it agrees for paying, The digital data regenerative apparatus characterized by having the accounting means charged to an operator, and a playback means to reproduce the superdistribution contents of which encryption was canceled when directions of the purport of a countervalue on which it agrees for paying are received from an operator.

[Claim 10] By being contents packaging equipment which creates the package containing two or more contents, and encoding the candidate for distribution by different method A coding means to obtain two or more contents from which the quality at the time of playback differs, and a rank means to rank each contents according to the height of playback quality, A conversion table storing means to store the conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, Contents packaging equipment characterized by having a packing means to generate the package containing said two or more enciphered contents.

[Claim 11] Said conversion table storing means is contents packaging equipment according to claim 10 characterized by storing by making said rank information and cryptographic key, and cryptographic algorithm into a group so that a code with high safety may be used for the contents reproduced in said high quality.

[Claim 12] While being contents packaging equipment which creates the package containing two or more contents and obtaining the contents for sample offer by encoding the part for distribution encoding the remaining part for distribution -- difference -- with a coding means to obtain contents a rank predetermined to the contents for sample offer -- giving -- difference -- with a rank means to give a higher rank to contents Two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank are made into the group. In one group A predetermined rank is matched. For another side to construct A conversion table storing means to store the conversion table matched with the rank higher than the predetermined rank concerned, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, Contents packaging equipment characterized by having a packing means to generate the package containing said two or more enciphered contents.

[Claim 13] Are the contents regenerative apparatus which takes out contents from a package and is reproduced, and the engine performance of the hardware of a regenerative apparatus is evaluated. An evaluation means to compute the rank estimator which shows the engine performance of the hardware concerned, and two or more rank estimators, A conversion table storing means to store the conversion table which the decode key which should be used for the encryption discharge processing, and the decode algorithm constructed, and matched ** when the hardware which has the engine performance corresponding to each rank estimator performed encryption discharge processing, An acquisition means to acquire the package whose each contains two or more contents by which encryption was made from the equipment exterior, While choosing the thing according to the rank estimator evaluated by the evaluation means among two or more decode keys which can be set to a conversion table, and a decode algorithm The contents regenerative apparatus characterized by having a discharge means to take out from a package the contents of which encryption should be canceled with this decode key and a decode algorithm, and to cancel encryption of the taken-out contents.

[Claim 14] The contents for sample offer obtained by encoding the part for distribution, It is the contents regenerative apparatus which takes out contents from the package containing contents and is reproduced. the difference which

encoded the remaining part for distribution and was obtained by enciphering in a cryptographic key and cryptographic algorithm with safety higher than the contents for sample offer -- An evaluation means to compute the rank estimator which evaluates the engine performance of the hardware of a regenerative apparatus and shows the engine performance of the hardware concerned, The decode key and decode algorithm of which encryption of the contents for sample offer can be canceled are matched with the low rank estimator. difference -- with a conversion table storing means to store the conversion table which matched with the high rank estimator the decode key and decode algorithm of which encryption of contents can be canceled An acquisition means to acquire the package whose each contains two or more contents by which encryption was made from the equipment exterior, While choosing the thing corresponding to the rank estimator evaluated by the evaluation means among two or more decode keys which can be set to a conversion table, and a decode algorithm the contents for sample offer from the acquired package, and difference -- the contents regenerative apparatus characterized by having a discharge means to take either of the contents out and to cancel encryption of the taken-out contents.

[Claim 15] The record medium characterized by recording the contents for sample offer enciphered in a predetermined cryptographic key and predetermined encryption algorithm, and the contents for sale which were

reproduced in quality higher than the contents for sample offer, and were enciphered in a cryptographic key and encryption algorithm with safety higher than said predetermined cryptographic key and said predetermined encryption algorithm.

[Claim 16] enciphering in a cryptographic key and encryption algorithm with safety higher than said predetermined cryptographic key and said predetermined encryption algorithm, after encoding the contents for sample offer obtained by enciphering in a predetermined cryptographic key and predetermined encryption algorithm after encoding the part for distribution, and the remaining part for distribution -- difference -- the record medium characterized by recording contents.

[Claim 17] The contents packaging equipment which creates the package containing two or more contents, It is the system which consists of a contents regenerative apparatus which takes out contents from a package and is reproduced. Said contents packaging equipment A coding means to obtain two or more contents from which the quality at the time of playback differs by encoding the candidate for distribution by different method, A rank means to rank each contents according to the height of playback quality, The conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents

of each rank is stored. In one group A predetermined rank is matched. For another side to construct A 1st conversion table storing means to store the conversion table matched with the rank higher than the predetermined rank concerned, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, It has a packing means to generate the package containing said two or more enciphered contents. Said contents regenerative apparatus An evaluation means to compute the rank estimator which evaluates the engine performance of the hardware of a regenerative apparatus and shows the engine performance of the hardware concerned, A 2nd conversion table storing means to store the conversion table which matched the decode key and decode algorithm which should be used for the encryption discharge processing when the hardware which has the engine performance corresponding to two or more rank estimator and each rank estimator performed encryption discharge processing, An acquisition means to acquire the package whose each contains two or more contents by which encryption was made from the equipment exterior, While choosing the thing according to the rank estimator evaluated by the evaluation means among two or more decode keys which can be set to a conversion table, and a decode algorithm The system characterized by having a discharge means to take out from a package the contents of which encryption

should be canceled with this decode key and a decode algorithm, and to cancel encryption of the taken-out contents.

[Claim 18] A computer with the storing section which stores at least one or more contents The selection step which is the record medium which can be read, and chooses the contents as superdistribution contents when what should charge record to the playback or other record media exists in said one or more contents, So that the playback about selected superdistribution contents or record to other record media may be prevented, while accounting is not performed The 1st encryption step which enciphers superdistribution contents based on the 1st cipher system, The generation step which generates a superdistribution header including the key information of which encryption of superdistribution contents is made to cancel, The generated superdistribution header is enciphered based on the 2nd cipher system with safety higher than said 1st cipher system. If the 2nd encryption step given to superdistribution contents and a superdistribution header are given The record medium which is characterized by recording the record program to which the procedure which consists of a record step recorded on a record medium by using one or more contents as digital data is made to carry out to a computer and in which computer reading is possible.

[Claim 19] They are the 1st record medium and the record medium which a computer with the loading section loaded with either of the 2nd record medium

can read. The read-out step which will read this from the 1st record medium if the loading section is loaded with the 1st record medium with which the superdistribution contents enciphered in order to prevent what recorded on other record media while accounting is not performed were recorded, The presentation step which shows an operator the countervalue to record to the 2nd record medium of superdistribution contents, The discharge step of which encryption of the superdistribution contents read from the 1st record medium is canceled when the actuation which the reception step which receives the actuation from an operator, and the reception step received is actuation of the purport of a countervalue on which it agrees for paying, If it is loaded with the accounting step charged to an operator, and the 2nd record medium which serves as an archive destination of superdistribution contents at the loading section when directions of the purport of a countervalue on which it agrees for paying are received from an operator The record medium which is characterized by recording the record program to which the procedure which consists of a record step recorded on the 2nd record medium of an archive destination by using as digital data the superdistribution contents of which encryption was canceled is made to carry out to a computer and in which computer reading is possible.

[Claim 20] It is the record medium which a computer with the loading section

loaded with a record medium can read. If the loading section is loaded with the record medium with which the superdistribution contents which accounting is required for the playback, and are enciphered in order to prevent playback while accounting is not performed were recorded The read-out step which reads superdistribution contents, and the presentation step which shows an operator the countervalue to playback of superdistribution contents, The reception step which receives the actuation from an operator, and the discharge step of which encryption of superdistribution contents is canceled when the actuation which the reception step received is actuation of the purport of a countervalue on which it agrees for paying, The accounting step charged to an operator when directions of the purport of a countervalue on which it agrees for paying are received from an operator, The record medium which is characterized by recording the playback program to which the procedure which consists of a playback step which reproduces the superdistribution contents of which encryption was canceled is made to carry out to a computer if accounting is performed to an operator and in which computer reading is possible.

[Claim 21] It is the record medium which a computer with the conversion table storing section which stores the conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank can read. The coding step

which obtains two or more contents from which the quality at the time of playback differs by encoding the candidate for distribution by different method, The rank and ** step which rank each contents according to the height of playback quality, The encryption step which enciphers the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, The record medium which is characterized by recording the packaging program to which the procedure which consists of a packing step which generates the package containing said two or more enciphered contents is made to carry out to a computer and in which computer reading is possible.

[Claim 22] It is the record medium which a computer with the storing section which stores the conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank can read. While obtaining the contents for sample offer by encoding the part for distribution encoding the remaining part for distribution -- difference -- with said coding step which obtains contents a rank predetermined to the contents for sample offer -- giving -- difference -- with the rank step which gives a higher rank to contents The encryption step which enciphers the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table,

The record medium which is characterized by recording the packaging program to which the procedure which consists of a packing step which generates the package containing said two or more enciphered contents is made to carry out to a computer and in which computer reading is possible.

[Claim 23] When the hardware which has the engine performance corresponding to two or more rank estimator and each rank estimator performs encryption discharge processing, Are the record medium which the computer which has the storing section which stores the conversion table which matched the decode key and decode algorithm which should be used for the encryption discharge processing can read, and the engine performance of the hardware of a computer is evaluated. The evaluation step which computes the rank estimator which shows the engine performance of the hardware concerned, The acquisition step which acquires the package whose each contains two or more contents by which encryption was made from the computer exterior, While choosing the thing according to the rank estimator evaluated by the evaluation step among two or more decode keys which can be set to a conversion table, and a decode algorithm The contents of which encryption should be canceled with this decode key and a decode algorithm are taken out from a package. The record medium which is characterized by recording the packaging program to which the procedure which consists of a discharge step of which encryption of the

taken-out contents is canceled is made to carry out to a computer and in which computer reading is possible.

[Claim 24] A computer with the storing section which stores at least one or more contents which should be recorded on a record medium It is the record approach which records the digital data containing contents on a record medium. The selection step which chooses the contents as superdistribution contents when what should charge record to the playback or other record media exists in said one or more contents, So that the playback about selected superdistribution contents or record to other record media may be prevented, while accounting is not performed The 1st encryption step which enciphers superdistribution contents based on the 1st cipher system, The generation step which generates a superdistribution header including the key information of which encryption of superdistribution contents is made to cancel, The generated superdistribution header is enciphered based on the 2nd cipher system with safety higher than said 1st cipher system. The record approach characterized by making the procedure which consists of the 2nd encryption step given to superdistribution contents and a record step which will be recorded on a record medium by using one or more contents as digital data if a superdistribution header is given perform to a computer.

[Claim 25] Said record approach is applied to a computer with the loading

section which loads with any of the 1st record medium and the 2nd record medium they are. It is the record approach which records the digital data containing the superdistribution contents recorded on the 1st record medium on the 2nd record medium. The read-out step which will read this from the 1st record medium if the loading section is loaded with the 1st record medium with which the superdistribution contents enciphered in order to prevent what recorded on the 2nd record medium while accounting is required for record to the 2nd record medium and accounting is not performed were recorded, The presentation step which shows an operator the countervalue to record to the 2nd record medium of superdistribution contents, The discharge step of which encryption of the superdistribution contents read from the 1st record medium is canceled when the actuation which the reception step which receives the actuation from an operator, and the reception step received is actuation of the purport of a countervalue on which it agrees for paying, If it is loaded with the accounting step charged to an operator, and the 2nd record medium which serves as an archive destination of superdistribution contents at the loading section when directions of the purport of a countervalue on which it agrees for paying are received from an operator The record approach characterized by making the procedure which consists of a record means to record on the 2nd record medium of an archive destination by using as digital data the

superdistribution contents of which encryption was canceled perform to a computer.

[Claim 26] It is the playback approach which reproduces the digital data which is applied to a computer with the loading section loaded with a record medium, and is recorded on the record medium. The read-out step which will read this if the superdistribution contents enciphered in order to prevent playback while accounting is required for the playback and accounting is not performed to the record medium with which the loading section was loaded are recorded, The presentation step which shows an operator the countervalue to playback of superdistribution contents, The reception step which receives the actuation from an operator, and the discharge step of which encryption of superdistribution contents is canceled when the actuation which the reception step received is actuation of the purport of a countervalue on which it agrees for paying, The accounting step charged to an operator when directions of the purport of a countervalue on which it agrees for paying are received from an operator, The playback approach characterized by making the procedure which consists of a re-**** playback step the superdistribution contents of which encryption was canceled perform to a computer if accounting is performed to an operator.

[Claim 27] It is applied to a computer with the conversion table storing section which stores the conversion table which made the group two or more ranks, and

the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank. By being the contents packaging approach which creates the package containing two or more contents, and encoding the candidate for distribution by different method The coding step which obtains two or more contents from which the quality at the time of playback differs, and the rank and ** step which rank each contents according to the height of playback quality, The encryption step which enciphers the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, The contents packaging approach characterized by making the procedure which consists of a packing step which generates the package containing said two or more enciphered contents perform to a computer.

[Claim 28] It is applied to a computer with the storing section which stores the conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank. While being the contents packaging approach which creates the package containing two or more contents and obtaining the contents for sample offer by encoding the part for distribution encoding the remaining part for distribution -- difference -- with said coding step which obtains contents a rank predetermined to the contents for sample offer --

giving -- difference -- with the rank and ** step which give a higher rank to contents The encryption step which enciphers the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, The contents packaging approach characterized by making the procedure which consists of a packing step which generates the package containing said two or more enciphered contents perform to a computer.

[Claim 29] When the hardware which has the engine performance corresponding to two or more rank estimator and each rank estimator performs encryption discharge processing, It is applied to a computer with the storing section for the conversion table which matched the decode key and decode algorithm which should be used for the encryption discharge processing. Are the contents playback approach which takes out contents from a package and is reproduced, and the engine performance of the hardware of a computer is evaluated. The evaluation step which computes the rank estimator which shows the engine performance of the hardware concerned, The acquisition step which acquires the package whose each contains two or more contents by which encryption was made from the computer exterior, While choosing the thing according to the rank estimator evaluated by the evaluation step among two or more decode keys which can be set to a conversion table, and a decode algorithm The playback

approach characterized by making the procedure which consists of a discharge step of which the contents of which encryption should be canceled with this decode key and a decode algorithm are taken out from a package, and encryption of the taken-out contents is canceled perform to a computer.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the record medium which recorded the contents which make the start the digitized music work, the equipment which records contents on a record medium, the equipment which reproduces the contents currently recorded on the record medium, the equipment which carries out packaging of two or more contents, the record medium in which computer reading is possible, the record approach, the playback approach, and the packaging approach.

[0002]

[Description of the Prior Art] (The 1st conventional technique) It argues about how there should be any selling gestalt of a next-generation music work briskly between major concert companies, the sound appliance maker, and the well-informed person. The selling gestalt of the present music work is a gestalt of

recording the music work of various genres, such as pop, a lock, and a classic, on record media, such as CD and a magnetic tape, and selling it, and it can be said that the life style of purchasing the record medium sold in this way, and appreciating a music work has permeated all over the world.

[0003] As a selling gestalt which opposes the selling gestalt using a record medium, the selling gestalt called an electronic music distribution attracts many attentions. An electronic music distribution performs charged distribution of a music content (contents say the thing of the digitized work and especially a music content says the thing of the digitized music work) on the Internet which shows rapid spread in recent years. The special feature of this electronic music distribution is the point that accounting to the proposal of sale of a music content and those who purchased the music content is performed according to electronic commerce (Electronic Commerce). That is, in this electronic music distribution, the concert company is introducing various contents to the homepage which self opened, and a consumer can search various contents by accessing the homepage of each concert company. When there are favorite contents, a consumer notifies this concert company of the purchase demand of contents, Operator ID, etc. A concert company can settle the purchase price of contents based on the bank account corresponding to the number of the credit card beforehand notified by the operator. After such settlement of accounts, a

consumer can download contents to the computer which the consumer owns, and can obtain his favorite contents.

[0004] Thus, in an electronic music distribution, since it downloads according to interactive selection actuation, it sets to the homepage to which whenever [cognitive] sells the contents of a high newly released piece of music, for example, and if the contents of other scores of the singer who sings the contents of other scores of the artist who wrote the lyrics for and composed the contents of the newly released piece of music, and the contents of the newly released piece of music are introduced, a score besides these can be sold to a consumer. That is, it is statistically clear that the consumer's who is going to purchase a certain artist's newly released piece of music an interest strong against the score with which the artist is related is shown, and he can promote such two or more related scores efficiently in the electronic music distribution.

[0005] (The 2nd conventional technique) As the 1st conventional technique described, there are various things at first in the distribution gestalt of a music content about the selling gestalt using communication lines which used the record medium, such as a selling gestalt and the Internet. Even if it says at a record medium and a word, there is a class of DVD-Audio, CD, etc. of record media, and each of these is recording the music content on them in the condition of having encoded with a different coding method. Moreover, there are also

many opportunities for a music content to be distributed, by being broadcast in broadcast waves, such as satellite broadcasting service and a cable TV, besides such a selling gestalt. Although it is a principle that these distribution is performed for counter value, it may be offered gratuitously as a sample in order to raise the notability of a music content.

[0006] When a music work is distributed with various gestalten like a record medium, a broadcast wave, and a communication line, even if the number of the music works which should be distributed even if is one, the side which distributes a music work must create and distribute the music content of the gestalt according to each distribution gestalt. Here, it is based on the following reasons that it must encode by different coding method. That is, since the height of the existence of a copyright protection feature and the safety of a cryptographic key differs in the regenerative apparatus which has already spread through each household, and the regenerative apparatus which is spreading from now on from the height of the playback quality of the music content at the time of playback for every regenerative apparatus, even if it transmits a music content to it uniformly by the same coding method, it is because a copyright protection feature is not utilized at all or there is a possibility that the ability to regenerate with which the regenerative apparatus is originally equipped cannot be demonstrated.

[0007] If the regenerative apparatus with which the copyright protection feature

is already fixed exists, I can think that what is necessary is just to encipher the music content distributed with all gestalten in a cryptographic key with high safety. However, encryption according to a cryptographic key with such high safety also for reproducing the contents of quality low to sample offer if the music content reproduced only in quality low such since what is necessary is for there to be some which are distributed to a music content for the purpose of the object for sample offer etc. and the improvement in notability, and to just be reproduced in quality with such a low music content is also uniformly enciphered in a cryptographic key with high safety must be solved. Now, the regenerative apparatus which does not have the decode capacity to cancel encryption with high safety will become impossible [reproducing the contents for sample offer], and its opportunity for the contents for sample offer to be reproduced will decrease. Thus, if the opportunity for the contents for sample offer to be reproduced decreases, advertising activities of aiming at sales promotion broadly by sample offer of a music content will lose an original target. Creating and distributing the music content of a gestalt according to each distribution gestalt by the above reason was performed inevitably.

[0008]

[Problem(s) to be Solved by the Invention] By the way, infrastructures for becoming a problem in the 1st conventional technique to realize an electronic

music distribution are the present condition and the point that a consumer is burdened with various burdens, in order to be unable to say that it is fixed enough but for a consumer to receive a music content in an electronic music distribution. Although a typical thing is the high speed line which can transmit the music content which has the data size of several megabytes in a short time among the infrastructures made indispensable because of implementation of an electronic music distribution here, the general Internet user uses the Internet by accessing a server through a public line. As for the transmission speed of the public line which the general Internet user uses, it is common that it is much less than the transmission speed of a high speed line. Thus, since communication link time amount turns into long duration when the general Internet user downloads two or more contents to coincidence as mentioned above through a low speed public line, a consumer will pay a great communication link tariff to a communication link firm. When extreme, it is possible that the way of a communication link tariff becomes high from the tariff which a consumer pays to a concert company about the purchase of contents. Thus, if a consumer is burdened with a great tariff, the volition of the consumer who is going to use an electronic music distribution will be depressed in spirits. Since the time amount which the transfer in a public line takes becomes very long when transmitting two or more contents, increasing also on the problem of this tariff side and

feeling uneasy is the point of irritating for fun those who wished the purchase of contents. Thus, if a transfer of contents excels, those who wished the purchase of contents may cancel the purchase of contents in the middle of download of two or more contents.

[0009] But in the selling gestalt using a record medium, when it is going to sell the contents of a related score like an electronic music distribution, a selling point, the selling price, etc. are printed about such a related score in the jacket enclosed by the case which contained the record medium, and the classic technique of recommending the purchase of a related score must be taken in it. A consumer receives a related score by going to the retail store of contents, in order to purchase the related score, and purchasing the record medium with which the related score was recorded, when the contents of printing of such a jacket are seen and being got interested in a related score.

[0010] Various costs concerning manufacture and circulation of a record medium are appropriated for the retail price of the record medium currently sold to the retail store here. Therefore, since it is necessary to pay the retail price for which various costs concerning manufacture and circulation of these record media were appropriated about each of two contents when it is going to purchase the both sides of the record medium with which the newly released piece of music was recorded, and the record medium with which the related score was recorded,

a consumer will pay a comparatively high-priced tariff.

[0011] Moreover, in the selling gestalt using the present record medium, in order for a consumer to receive a related score, the volition which is going to purchase such a related score by the time the consumer itself has to go to the retail store of a record medium specially, and a consumer cannot purchase a related score freely but it goes to the retail store of a record medium may be lost. Moreover, in the 2nd conventional technique, since the feeder of a music content needs to encode by different coding method according to a distribution gestalt, the more there are many contents encoded, the more he is the point that the feeder of a music content senses great stress for management and distribution of these music contents. Thus, if the number of the contents encoded increases, stress will be sensed, for example because the probability of a misdelivery-of-mail cloth, such as distributing the contents for sale and the contents for sample offer accidentally, also becomes high. If such a misdelivery-of-mail cloth arises, the contents for sale will flow into a public place, and if those all are not collected, the feeder of a music content will wear a great blow economically.

[0012] the music content relevant to this music content to the consumer who purchased a certain music content even if the infrastructure for realizing an electronic music distribution had not fixed the 1st purpose of this invention -- a low price -- in addition -- and it is offering the record medium which can be sold

easily. The 2nd purpose of this invention is offering the contents packing equipment which can distribute the music content to these uniformly, even if the height of the existence of a copyright protection feature and the safety of a cryptographic key and the height of the playback quality of the music content at the time of playback are the cases where it differs for every regenerative apparatus.

[0013]

[Means for Solving the Problem] The 2nd contents which the 1st purpose of the above is the 1st contents and contents from which the 1st contents differ, and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make the encryption in the 2nd contents cancel is included. It is attained by the record medium by which the header enciphered with the 2nd cipher system which is a cipher system with which discharge of the encryption is performed is recorded only when the 2nd key information beforehand distributed to predetermined equipment is used.

[0014] A coding means to obtain two or more contents from which the quality at the time of playback differs when the 2nd purpose encodes the candidate for distribution by different method, A rank means to rank each contents according to the height of playback quality, A conversion table storing means to store the conversion table which made the group two or more ranks, and the

cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, It is attained by contents packaging equipment equipped with a packing means to generate the package containing said two or more enciphered contents.

[0015]

[Embodiment of the Invention] The operation gestalt about the record medium concerning this invention, a regenerative apparatus, and a recording device is explained. In addition, since explanation will become remarkably complicated if one operation gestalt tends to explain a record medium, a regenerative apparatus, and a recording device, the above-mentioned contents shall be explained according to an individual in the 6th operation gestalt from the 1st operation gestalt.

[0016] (The 1st operation gestalt) The 1st operation gestalt explains the record medium used for the selling application of a music content. The music content for the purpose of selling is recorded on the record medium used for the selling application of a music content, and sale of contents is made by transferring this record medium for counter value. There are two types of record media of such a selling application. The 1st type records the music content aiming at sale on

Enhanced-CD. It has the physical structure as the usual CD (CD-DA) with the same inner circumference section, and the disk which has the physical structure as CD-ROM with the same periphery section, and had the function of both CD and CD-ROM is called Enhanced-CD. The appearance of this Enhanced-CD is shown in drawing 1 (a), and the physical structure of Enhanced-CD is shown in drawing 1 (b). In drawing 1 (a), the inner circumference section of Enhanced-CD is called the CD-DA section, and the periphery section is called the CD-ROM section. When these CD-DA section and the CD-ROM section are considered functionally, the CD-DA section is the contents field 1 where the music content 3 is recorded, and the CD-ROM section is the added value field 2 which recorded the data which raise the added value of this record medium. This record medium for sale is used for the application which sells the music content recorded on this contents field 1.

[0017] The record medium of the selling application of the 2nd type is DVD-AUDIO on which the music content 3 for the purpose of selling was recorded. The appearance of this DVD-AUDIO is shown in drawing 2 (a), and the logical format is shown in drawing 2 (b). The CD-DA section shown in Enhanced-CD and the CD-ROM section are recorded on this DVD-AUDIO to not existing by the file with each of the selling purpose contents 3, the playback control script 4, the still picture data 5, and a container 6 accessible in a personal

computer. Thus, although the point recorded by the file differs from Enhanced-CD, functional DS is the same as that of Enhanced-CD, and consists of a contents field 1 and an added value field 2. Moreover, the point that a music content 3 is recorded on the contents field 1 in DVD-AUDIO, and the data which raise the added value of this record medium to the added value field 2 are recorded is also the same as that of Enhanced-CD. It is the point that the music content 3 for the purpose of [which is recorded by the contents field 1 of DVD-AUDIO to the difference from Enhanced-CD being recorded as it is, without also giving encryption / what / for the selling purpose contents 3] selling is enciphered at the contents field 1 of Enhanced-CD using the identification information of a DVD-AUDIO proper.

[0018] Like the usual CD, these two types of record medium for sale is contained by the plastics case of dedication, where a jacket and a musical score card are enclosed. Drawing 3 is drawing showing the plastics case of the dedication which contained the record medium for sale. It turns out that the photograph about music name:OOO is mainly printed in the music name of the contents currently recorded on the contents field 1 here as temporarily shown in the jacket of music name:OOO, then the record medium for sale at drawing 3 .

[0019] By the above explanation, it became clear that the contents field 1 and the added value field 2 exist in the both sides of Enhanced-CD and DVD-AUDIO.

Then, the contents of record of the added value field 2 are explained. The contents of record of the added value field 2 are shown in the right column of drawing 1 (b) and drawing 2 (b). As shown in this Fig., in the added value field 2, it turns out that the playback control script 4, the still picture data 5, and a container 6 are recorded.

[0020] When equipment with a display function is loaded with the record medium for this sale, the playback control script 4 is the information which described the contents displayed on the dialogue screen of this equipment, and is described in the Macromedia Director format and the HTML format. here -- a Macromedia Director format -- the utilization time of the general-purpose authoring software of MS-Windows/MacOS -- description of an authoring procedure -- business -- **** -- a format -- it is -- a HTML format is a format by which the object for ** is carried out to description of the Internet browser.

[0021] The still picture data 5 are the static image which should be displayed in the dialogue screen reproduced in the playback control script 4. Although these playback control scripts 4 and the still picture data 5 exist also in conventional Enhanced-CD, as for the still picture data 5 and the playback control script 4 in this operation gestalt, a conventional thing and the conventional contents of a display differ from each other. Namely, although the words of the selling purpose contents 3, a promotion image and a fan club, newly-released-piece-of-music

guidance, etc. display the information relevant to the selling purpose contents 3 on the conventional still picture data 5 and the conventional playback control script 4, the still picture data 5 and the playback control script 4 in this operation gestalt display on the above-mentioned equipment the information which recommends purchase and the playback of a music content which are different in the selling purpose contents 3.

[0022] For example, if it is the newly released piece of music of a popular artist with the selling purpose contents 3, the playback control script 4 in this operation gestalt will recommend purchase and playback of the hit song the popular artist's past. It is shown clearly by subsequent explanation what the music content to which purchase and playback are recommended in these playback control script 4 is.

[0023] Then, the container 6 in the added value field 2 included to the both sides of Enhanced-CD and DVD-AUDIO is explained. The DS of a container 6 is shown in drawing 4 . In this Fig., a container 6 consists of an encryption header 7 and encryption contents 8, the encryption header 7 contains the superdistribution header 9, and the encryption contents 8 contain the superdistribution contents 10.

[0024] here -- "a superdistribution" -- Emeritus Professor University of Tsukuba Mr. woods Ryoichi -- ** -- it is the circulation gestalt of the digital content to recite.

In a superdistribution, a digital content circulates, where the superdistribution header defined beforehand is given. At this superdistribution header, the countervalue information about the detail of the countervalue which shows the rightful claimant who should deal in a countervalue is describing, and tariff liquidation is performed, when a consumer wishes use of this digital content, and the device which a consumer owns interprets these rightful claimant information and countervalue information and creates use record.

[0025] The superdistribution header 9 and the superdistribution contents 10 are contained in the container 6 in the format on condition of such a superdistribution, i.e., a superdistribution format. Thus, the superdistribution contents 10 contained in the condition of having been enciphered in the container 6 are just music contents to which purchase and playback are recommended in the still picture data 5 and the playback control script 4.

[0026] Since information important in order to carry out a superdistribution to insurance, such as rightful claimant information and countervalue information, is shown in the superdistribution header 9 as mentioned above, it is necessary to prevent malfeasances, such as an alteration of this, efficiently. Therefore, the superdistribution header 9 in this operation gestalt includes the data area enciphered based on the cipher system adapting a public-key-encryption algorithm (in addition, the superdistribution header 9 whole may be enciphered.).

The following sentences explain as what the superdistribution header 9 whole is enciphered as. . It is known widely that there are generally classes of public key encryption, such as a elliptic curve cryptosystem and RSA cryptograph (Rivest, Shamir, Adleman encryption). Since it is necessary to use a different decode key from the public key used for encryption in order to decode the data enciphered using these public keys, it is said that safety of a public key is very high.

[0027] However, a public key is not only used for the cipher system of public key application used in case the superdistribution header 9 is enciphered in this operation gestalt, but the following points are improved. That is, in the cipher system of the public key application in this operation gestalt, the decode key for solving encryption of the data area in the superdistribution header 9 is beforehand distributed to the predetermined dedicated device, and when this dedicated device is loaded with the record medium for sale, encryption of the superdistribution header 9 is canceled. In case this dedicated device is connected to the communication line, encryption of the superdistribution header 9 tends to be canceled in this operation gestalt and superdistribution contents tend to be reproduced, or in case superdistribution contents are recorded on other record media, the dedicated device concerned performs accounting through a communication line so that the rightful claimant about superdistribution contents may get a just countervalue. In addition, when you are going to make it

record various superdistribution contents on the record medium for sale, a different public key is used about each superdistribution header of superdistribution contents. On the other hand, a dedicated device decodes this superdistribution header using a common decode key, even if enciphered using the public key with which those superdistribution headers differ. Moreover, although explained as what performs accounting at the time of setting in this operation gestalt, and a dedicated device reproducing or buying superdistribution contents through a communication line, accounting information is recorded on another record media, such as an IC card, and another equipment may perform the settlement of accounts about accounting information. Moreover, another equipment may perform accounting by the prepaid card.

[0028] Since the decode key for canceling encryption of the superdistribution header 9 is formed in the dedicated device and does not exist on the record medium for sale, even if a person with malice tries to acquire the record medium for sale and cancel encryption of this superdistribution header 9 using an inaccurate device, the probability for that encryption to be canceled is very low. Thus, since it is very difficult to cancel encryption of the superdistribution contents 10 unlawfully, the commercial transaction of the superdistribution contents 10 is carried out to insurance.

[0029] In addition, if the music name of the superdistribution contents 10 is made

into ******, as shown in drawing 3 , no contents about ****** are printed by the jacket of the record medium for sale. This is for ordinary consumers to prevent mistaking saying "Whether the superdistribution contents 10 are supplied gratuitously to those who purchased the selling purpose contents 3."

[0030] Then, the contents of the superdistribution header 9 are explained, referring to drawing 4 . In drawing 4 , the stage of most right-hand side shows the contents of the superdistribution header 9. The superdistribution header 9 consists of content ID 11, purchase conditions 12, and a decode key 13 so that he can understand also from here. Information for content ID 11 to discriminate the superdistribution contents 10 from other contents is described. Since the superdistribution contents 10 are music contents, identification information, such as ISRC (International Standard Recording Code), is described as content ID 11. ISRC is ID information on the proper uniquely assigned for every music here, and it is constituted by a country code (two ASCII characters), a record year (double digits), and the serial number (five digits).

[0031] The information concerning [the purchase conditions 12] the purchase conditions of contents is described. Here, an example of the purchase conditions 12 is shown in drawing 5 . In drawing 5 , a refreshable upper limit is integrally described by the "count of playback authorization" column. When a digital output terminal shows whether the digital output which minded this digital output

terminal the ********** case is permitted at a dedicated device and it permits "the count of digital output authorization", that count of an output is described by the integral value.

[0032] The time amount which the "playback authorization time amount" column permits playback of contents, i.e., reproducible time amount, is described. The date when the "playback authorization date" column permits playback of contents is described. When the date when playback was permitted passes, playback of the contents can be performed. The "accounting information" column includes the information which shows the price at the time of acquisition of the superdistribution contents 10, or the price at the time of playback. Here, in case the price at the time of acquisition records the superdistribution contents 10 in a container 6 on other record media, it means the price with which an operator is burdened, and the price at the time of playback expresses the price according to the count of playback of a specific charge 10, i.e., the superdistribution contents in a container 6. In electronic commerce, it is treated as a purchase application form with a signature, and, as for this accounting information, the owner of the record medium for sale means applying for the purchase of the superdistribution contents 10 in electronic commerce, as for this and a dedicated device transmitting Operator ID to the host computer in an accounting center. That is, the dedicated device loaded with a record medium transmits Operator ID

and this accounting information to the accounting center of a concert company through a communication line, when the operator has agreed on playback or acquisition of the superdistribution contents 10. On the other hand, since the credit card number is registered beforehand and learning of an operator's bank account corresponding to this card number has been beforehand carried out to the accounting center of a concert company, if Operator ID is transmitted, in it, the purchase price of contents will be settled by pulling down the price shown in accounting information from the bank account corresponding to the credit card number of the operator of that transmitting origin.

[0033] The decode key 13 is a decode key for decoding the superdistribution contents 10. The superdistribution contents 10 are music contents of a LPCM (Linear Pulse Code Modulation) format, an AAC (Advanced Audio Coding) format, and a DTS (Digital Theater System) format, and are enciphered with the block cipher system. A block cipher divides contents into every fixed die length (block length) of a certain, and means the approach of enciphering in the block unit, and DES (64 bits of block lengths are fixed), RC5 (the block length is adjustable), etc. are equivalent to this. Since the key for decrypting with the enciphered key in this block cipher system is the same, there is no safety highly like a public key. Although the decode key 13 must come to hand to cancel encryption of the superdistribution contents 10, since the decode key 13 exists in

the superdistribution header 9 firmly enciphered with the cipher system of public key application, safety is high and it is very difficult to cancel encryption of the superdistribution contents 10 unlawfully. The superdistribution contents 10 will be firmly protected as a result.

[0034] Thus, since the purchase conditions 12 about the purchase of the superdistribution contents 10 etc. are included in the superdistribution header 9 enciphered with the public key with high safety, they become very difficult [the alteration of accounting information, or decode of the superdistribution header 9]. Moreover, what is necessary is to cancel encryption of the superdistribution header 9, to take out the decode key 13 and just to cancel the superdistribution contents 10 using the decode key 13, in order to obtain the superdistribution contents 10, since the superdistribution contents 10 are not enciphered with a public key but only the superdistribution header 9 is enciphered with the public key. Since acquisition and the time amount which becomes reproducible are short and it ends after the part which should cancel encryption directs acquisition and playback of short **** and the superdistribution contents 10, since the part enciphered by the public key application method is limited to a part for a header unit, those who wished the superdistribution contents 10 are not irritated for fun. Since it is thought that the time amount which this discharge takes becomes very shorter than the time amount which download of the music content in an

electronic music distribution takes, an operator can appreciate immediately the superdistribution contents 10 which wished acquisition or playback.

[0035] Then, the management information about the selling purpose contents, a superdistribution header, and superdistribution contents is explained. Although the selling purpose contents are managed in the management information in CD and DVD-AUDIO here, a superdistribution header and superdistribution contents are not managed in such management information. Thus, since the selling purpose contents are managed in the management information in CD and DVD-AUDIO, it is recognized by a CD player and the DVD-AUDIO player (this does not mean the digital data regenerative apparatus 400 mentioned later) as music, and is reproduced, but since it is not managed in such management information, a superdistribution header and superdistribution contents are recognized by a CD player and the DVD-AUDIO player as music, and are not reproduced. If, as for this, a CD player and a DVD-AUDIO player tend to reproduce a superdistribution header and superdistribution contents as it is like the selling purpose contents, since a CD player and a DVD-AUDIO player will not be able to decode a superdistribution header and superdistribution contents but meaningless and jarring voice will be outputted, it is for a superdistribution header and superdistribution contents to avoid being reproduced like the selling purpose contents such. It replaces with the management information in such CD

and DVD-AUDIO, and it is managed in the management information of the proper for distinguishing self from the selling purpose contents, and when a dedicated device reads a superdistribution header and superdistribution contents, the recording start location-record termination location about a superdistribution header and superdistribution contents is pinpointed to a superdistribution header and superdistribution contents in the management information of this proper.

[0036] Then, it is shown clearly how these selling purpose contents 3 and the superdistribution contents 10 spread round a consumer, or how the superdistribution of the superdistribution contents 10 is performed, referring to drawing 6 . Drawing 6 is drawing showing how the selling purpose contents 3 in this operation gestalt and the superdistribution contents 10 circulate. In drawing 6 , the record medium for sale is manufactured, when the digital data recording apparatus 100 installed in the direct management works of a concert company as shown in an arrow head y1 records the selling purpose contents 3, the playback control script 4, the still picture data 5, and a container 6 on a record medium 200. Thus, like the usual CD, the manufactured record medium 200 for sale is sold through distribution channels, such as transportation of a truck, at the shop front of a retail store, as shown in an arrow head y2. Ordinary consumers can purchase the record medium 200 for sale currently sold as

shown in an arrow head y3.

[0037] The consumer who purchased the record medium 200 for sale can appreciate the selling purpose contents 3 in the same style as the usual CD and DVD-AUDIO. That is, as shown in the arrow head y4 of this Fig., the selling purpose contents 3 can be appreciated by reproducing the regenerative apparatus of a pocket mold during a walk. The digital data recording apparatus 300 and the digital data regenerative apparatus 400 shall be installed in domestic [of a consumer] as a dedicated device connected to the communication line here. Among these, the digital data recording device 300 makes the superdistribution contents 10 currently recorded on the record medium 200 for sale record on other record media for counter value, and the digital data regenerative apparatus 400 reproduces the superdistribution contents 10 currently recorded on the record medium 200 for sale for counter value. Moreover, the still picture data 5 currently recorded on the record medium 200 for sale and the playback control script 4 display on these digital data recording apparatus 300 and a digital data regenerative apparatus the dialogue screen shown in drawing 8 . Drawing 8 is drawing showing an example of the dialogue screen displayed on the display screen of a regenerative apparatus by the playback control script 4 and the still picture data 5. The image m1 with which the dialogue screen in drawing 8 introduces the superdistribution contents

10, such as a situation of a live performance, The message m2 of a purport which recommends playback of the superdistribution contents 10, and the carbon buttons m3 and m13 which can specify the approval or refusal to the playback, The frame m4 of a playback price, and the character string m5 which described the purport which recommends the purchase of the score concerned, It turns out that the carbon buttons m6 and m16 which can specify the approval or refusal to the purchase, and the purchase price m7 of those are included, and it has become the contents which recommend an onerous purchase and onerous playback of the superdistribution contents 10. If a consumer does learning of what kind of superdistribution contents 10 are recorded in the container 6 of Enhanced-CD and it is interested in them on this dialogue screen, a consumer can buy these superdistribution contents 10 using the digital data recording apparatus 300, and can reproduce these superdistribution contents 10 using a digital data regenerative apparatus. When the superdistribution contents 10 are bought and the superdistribution contents 10 are reproduced, the digital data recording apparatus 300 and the digital data regenerative apparatus 400 transmit the accounting information which shows the required amount of accounting through a public line. The transmitted accounting information is transmitted to the host computer 600 installed in the accounting center of a music center.

[0038] Drawing 7 (a) - drawing 7 (d) are drawings showing signs that the copy from the record medium 200 for sale to the record medium of an acquisition application is performed, through the digital data recording device 300. DVD-RAM shall be used as a record medium of an acquisition application here. If the record medium 200 for sale and the record medium 650 of an acquisition application are set in the digital data recording device 300 in drawing 7 (a), as shown in drawing 7 (b), the operator of the digital data recording device 300 will copy the work currently recorded on the record medium 200 for sale to the record medium 650 of an acquisition application. Then, if DVD-RAM which is the record medium 650 of an acquisition application is ejected as shown in drawing 7 (c), acquisition of the superdistribution contents 10 will be completed. After such acquisition, if DVD-RAM is taken out from the cartridge of DVD-RAM, the contents recorded on DVD-RAM will be reproduced by using the DVD-Audio player of the mold corresponding to DVD-RAM. Here, the DVD-Audio player of the mold corresponding to DVD-RAM means the DVD-Audio player which can perform playback of not only a DVD-Audio disk but DVD-RAM.

[0039] In addition, with this operation gestalt, although the digital data recording device 300 recorded superdistribution contents on DVD-RAM, it may be recorded on a memory card. In the above superdistributions, the amount of accounting to the superdistribution contents 10 can be set up at a reasonable

price as compared with the retail prices of the selling purpose contents 3. Because, it is because such a distribution cost becomes entirely unnecessary that acquisition of the superdistribution contents 10 should just only cancel encryption to various distribution costs which start circulation of Enhanced-CD, such as a freight cost of Enhanced-CD and DVD-AUDIO, and DVD-AUDIO at the retail prices of the selling purpose contents 3 being added up.

[0040] As mentioned above, according to this operation gestalt, even if it is in the situation that the infrastructure for the electronic data distribution represented by the Internet etc. is not fixed, promotion of a related score etc. can sell an interactive music content with the gestalt near an electronic music distribution. In addition, although Enhanced-CD and DVD-AUDIO were used with this operation gestalt as a record medium which records music, hybrid type DVD-AUDIO (DVD-AUDIO, disk which had the function of DVD-ROM) may be used. Furthermore, although this operation gestalt explained as what records the container which contains superdistribution contents and a superdistribution header in the record medium of a selling application, the container which contains superdistribution contents and a superdistribution header in the record medium distributed freely may be recorded.

[0041] Above, explanation of the DS of the 1st operation gestalt recorded on the record medium of this invention, i.e., a superdistribution format, is finished.

(The 2nd operation gestalt) The 2nd operation gestalt is related with the digital data recording device 100 which records the data of a superdistribution format on a record medium. The configuration of the digital data recording device 100 concerning the 2nd operation gestalt is shown in drawing 9 . It realizes by installing the application program of dedication in a general-purpose personal computer, and the digital data recording device 100 of the 2nd operation gestalt is equipped with the input section 101, a control section 102, the encoding section 103, the contents storing section 104, a takeoff connection 105, the superdistribution contents encryption section 106, the superdistribution header encryption section 107, the selling purpose contents encryption section 108, the Records Department 109, and the proper information takeoff connection 110, and records superdistribution contents on the record medium 200 of a selling application. Henceforth, explanation about these components is given.

[0042] In addition, henceforth although [this operation gestalt / the candidate for record] it is a music content, it may not be restricted to this and image data, alphabetic data, or the data of such combination is sufficient. Moreover, as data which should be recorded on the record medium 200 of a selling application, with the 1st operation gestalt, although the playback control script 4 and the still picture data 5 were illustrated, since it differs from the chief aim of this operation gestalt, explanation is omitted about the procedure in which these are recorded.

[0043] It connects with pointing devices, such as a mouse and a keyboard, and the input section 101 receives directions of an operator. Here, with directions of an operator, directions of encoding of a music content or the encoded ejection demand of data is mentioned. A control section 102 interprets the demand of the input section 101, and directs it to the encoding section 103 which mentions encoding a music content later. Or it directs to the takeoff connection 105 which mentions too later taking out the music content currently recorded on the contents storing section 104 mentioned later.

[0044] The encoding section 103 encodes the fundamental tone currently recorded on the master tape which is not illustrated to the digital data of for example, a LPCM format, compresses it into an AAC format, and generates a music content. The content ID 11 shown in the 1st operation gestalt after that is generated. In addition, in the digital data recording device 100, the encoding section 103 is not indispensable. When requesting encoding of a music content from an external contractor and recording the encoded data on the contents storing section 104, it is because it becomes unnecessary [the encoding section 103].

[0045] The contents storing section 104 is a mass hard disk drive unit, and stores the music content obtained by encoding of the encoding section 103, and the content ID 11 shown in the 1st operation gestalt. A takeoff connection 105

takes out the content ID 11 shown in the 1st operation gestalt at the music content list obtained by encoding from the contents storing section 104 based on the directions from a control section 102.

[0046] The superdistribution contents encryption section 106 generates the encryption contents 8 by enciphering the superdistribution contents 10 using the decode key 13 explained with the 1st operation gestalt. Here, the operator of this digital data recording device 100 can set up the decode key 13 freely. The superdistribution header encryption section 107 obtains the encryption header 7 by combining the purchase conditions 12, the content ID 11, and the decode key 13 of data of the superdistribution format described by the operator, obtaining the superdistribution header 9, and enciphering this. Furthermore, it gives the encryption contents 8 as which the superdistribution contents encryption section 106 enciphered the generated encryption header 7, and a container 6 is obtained.

[0047] The record medium 200 for sale is DVD-AUDIO, and when the selling purpose contents 3 need to be enciphered based on the identification information of a record-medium proper, the proper information takeoff connection 110 takes out the identification information of the medium proper currently beforehand recorded at the time of manufacture of the record medium 200 of a selling application, and outputs it to the selling purpose contents

encryption section 108. In addition, the record medium 200 for sale is Enhanced-CD, and when the selling purpose contents 3 do not need to be enciphered, ejection does not perform identification information of a medium proper.

[0048] The selling purpose contents encryption section 108 enciphers the selling purpose contents 3 based on the identification information of a record-medium proper, when the record medium 200 for sale is DVD-AUDIO. In addition, the record medium 200 for sale is Enhanced-CD, and when the selling purpose contents 3 do not need to be enciphered, the selling purpose contents encryption section 108 does not encipher. In addition, since it is indicated by JP,5-257816,A about the technique enciphered based on the identification information of a medium proper, detailed explanation is omitted here.

[0049] The Records Department 109 records the container 6 generated by the superdistribution header encryption section 107 and the selling purpose contents enciphered in the second encryption section 108. The actuation is explained about the digital data recording apparatus constituted as mentioned above using the flow chart which shows the contents of processing of drawing 10 henceforth. In addition, about the following actuation, encoding of a fundamental tone shall be completed and two or more music contents shall already have been obtained by the encoding section 103 at the contents storing

section 104.

[0050] If a control section 102 is started, a control section 102 will wait for the selection of a thing which should be recorded on the record medium 200 of a selling application among two or more contents stored in the contents storing section 104 in step S1. If contents are chosen, in step S2, a control section 102 will wait the music content from an operator for the record directions to the record medium 200 of a selling application. There are record directions of the purport recorded for the purpose of sale and record directions of the purport recorded for the purpose of a superdistribution as record directions here. When there are record directions, a control section 102 judges record directions of the purport which it records for the purpose of selling in step S3, and record directions in it and a superdistribution format.

[0051] When an operator performs record directions of the contents of a selling application, in step S3, it is judged with record directions of the contents of a selling application having been made. In this case, a control section 102 shifts to step S8 from step S3, and judges whether the type of the record medium 200 of a selling application is DVD-AUDIO, or it is Enhanced-CD in step S8. If it is Enhanced-CD, it shifts to step S6 from step S8, and the ejection of the music content chosen as the takeoff connection 105 and content ID is directed, and the music content and content ID which were taken out are made to record on the

record medium 200 of a selling application. On the other hand, if it is DVD-AUDIO, it shifts to step S9 from step S8. While a control section 102 directs the ejection of a suitable music content and content ID to a takeoff connection 105 in step S9, the taken-out music content is handed over in the selling purpose contents encryption section 108. The selling purpose contents encryption section 108 directs the ejection of the identification information of the proper from the record medium 200 of a selling application to the proper information takeoff connection 110, and the proper information takeoff connection 110 which received this takes out the identification information of a proper from the record medium 200 of a selling application. Then, it shifts to step S10 from step S9, and the selling purpose contents encryption section 108 enciphers, using the identification information of the medium proper taken out by the proper information takeoff connection 110 as a cryptographic key. Then, it shifts to step S6 from step S10, and the Records Department 109 records the selling purpose contents and content ID which were enciphered in the selling purpose contents encryption section 108 on the record medium 200 of a selling application. Since the record medium 200 of a selling application was recorded for the selling purpose contents by processing from step S1 to step S6, actuation when record directions of superdistribution contents are made is explained.

[0052] When record directions are superdistribution formats, a control section

102 makes a takeoff connection 105 take out the selected music content and content ID, and makes it output content ID to the header encryption section 107, and the superdistribution contents encryption section 106 is made to output it to it. The superdistribution contents encryption section 106 generates encryption contents by enciphering the contents taken out in step S4. Furthermore, by making it encipher by combining content ID 11, the purchase conditions 12, and the decode key 13 with the superdistribution header encryption section 107 in step S5, a control section 102 makes the encryption header 7 generate, and generates a container 6 by making the encryption header 7 give the encryption contents 8. Then, it shifts to step S6 and the generated container 6 is made to record on the record medium 200 of a selling application. If record to a record medium is completed, supposing it will ask an operator whether end a record activity in step S7 and will end, the processing in this flow chart will be ended. If it continues, it will shift to step S1 from step S7. Since this will be chosen as superdistribution contents 10 and this will be enciphered, if a thing to be payment [countervalue] is in record to the playback or other record media among one or more contents which should be recorded on the record medium 200 of a selling application as mentioned above according to this operation gestalt, while accounting is not performed, the playback about the superdistribution contents 10 or record to other record media can be prevented.

[0053] Since the superdistribution header 9 containing the accounting information made to charge a dedicated device and the decode key 13 of which a dedicated device is made to cancel encryption of the superdistribution contents 10 after accounting is given to the superdistribution contents 10 when enciphering the superdistribution contents 10 and reproducing or buying the superdistribution contents 10, whenever playback of the superdistribution contents 10 or record to other record media is performed, a concert company can acquire a profit.

[0054] Above, explanation of the 2nd operation gestalt is finished.

(The 3rd operation gestalt) Next, explanation about the digital data recording device 300 is given as the 3rd operation gestalt. From the side face of acquisition of the superdistribution contents 10, if the internal configuration of the digital data recording apparatus 300 is described functionally, the internal configuration of the digital data recording apparatus 300 is shown in drawing 11 . Drawing 11 is drawing showing the internal configuration of the digital data recording device 300 of the 3rd operation gestalt. Originally the digital data recording apparatus 300 is a digital data recording apparatus of the mold corresponding to an electronic music distribution, and the download function 313 in an electronic music distribution, i.e., the communications department, receives contents from the Internet for counter value, and it has the function recorded on

the record medium 650 of an acquisition application. Since it is a mold corresponding to an electronic music distribution, the digital data recording device 300 has the communications department for communicating the Internet, and the accounting section for settling money on a communication line, when electronic commerce is performed in a communication line.

[0055] In drawing 11 , it realizes by generally installing the application program of dedication in a general-purpose personal computer, and the digital data recording device 300 of the 3rd operation gestalt is equipped with the input section 301, a display 302, a control section 303, a takeoff connection 304, the superdistribution header decryption section 305, the superdistribution contents decryption section 306, the proper information takeoff connection 307, the superdistribution contents re-encryption section 308, the Records Department 309, the accounting section 310, the accounting information storing section 312, the communications department 313, and the recording rate Management Department 314.

[0056] It connects with pointing devices, such as a mouse and a keyboard, and the input section 301 receives purchase directions of the music from an operator. With the purchase of the music in a "superdistribution", the action of "recording the data of a superdistribution format on another record medium" is included. Here, the action of a digital output terminal making a digital output perform for

these digital output terminals a ********** case at a digital data recording apparatus and a digital data regenerative apparatus is also included in "the purchase of music." It is because this record medium can be made to record the superdistribution contents 10 on it using this drive equipment if the drive equipment of another record medium is connected to such a digital output terminal. In this operation gestalt, the digital data recording apparatus 100 has the digital output terminal, and has connected the drive equipment of DVD-RAM through a cable.

[0057] A display 302 presents visually the information on the contents of the superdistribution contents 10, the frame of the countervalue at the time of purchasing this, etc. by displaying a dialogue screen based on the playback control script 4 and the still picture data 5 which are recorded on the record medium 200 of a selling application. A control section 303 interprets the directions of an operator inputted through the input section 301, and directs to other components. Or the next processing is directed according to the result which other components outputted. For example, if there are purchase directions of a related score from an operator, the ejection of the superdistribution contents 10 currently recorded on the record medium 200 of a selling application and the superdistribution header 9 will be directed to the takeoff connection 304 mentioned later.

[0058] A takeoff connection 304 takes out the container 6 currently recorded on the record medium 200 of the selling application shown in the 2nd operation gestalt. The superdistribution header decryption section 305 will decrypt using the decode key 13 to the encryption header 7 in the container 6 contained in it, if a takeoff connection 304 takes out a container 6. If the superdistribution header 9 is obtained by decode, the purchase conditions of the superdistribution contents 10 can be shown to an operator by referring to the content ID 11 contained in this, the purchase conditions 12, and the decode key 13. In addition, what is distributed from an accounting center is used for the decode key used in case a superdistribution header is decoded through the thing beforehand stored in the application program installed in the digital data recording device 300, or a communication line.

[0059] The superdistribution contents decryption section 306 will decrypt the encryption contents 8 using the decode key 13 contained in this, if the superdistribution header decryption section 305 decrypts the superdistribution header 9. The proper information takeoff connection 307 takes out the identification information of a medium proper from the record medium 650 of an acquisition application. Since the record medium 650 of an acquisition application is DVD-RAM, the information written to BCA (Burst Cutting Area) is used for it as identification information of a medium proper here. For every disk,

the identification information of this medium proper is unique, is information moreover recorded usually at the time of disk manufacture, and cannot be rewritten. Therefore, even if an operator with malice should reproduce the contents of the disk, since the identification information which becomes the basis of a decode key differs, it cannot decrypt, but it becomes possible to protect the copyright of data certainly.

[0060] The superdistribution contents re-encryption section 308 enciphers the superdistribution contents 10 which the superdistribution contents decryption section 306 decrypted based on the identification information of the record-medium 650 medium proper of the acquisition application which the proper information takeoff connection 307 took out. The Records Department 309 records the superdistribution contents 10 enciphered by the superdistribution contents re-encryption section 308 on the record medium 650 of an acquisition application.

[0061] If the accounting section 310 has the notice of termination of processing of the Records Department 309, from the purchase conditions 12 acquired when the superdistribution header decryption section 305 decoded the superdistribution header 9, it will compute the amount of accounting based on the accounting information by reading accounting information, and will include it in accounting information. The accounting information storing section 312 is

equivalent to the hard disk of a personal computer, and stores the accounting information containing the amount of accounting which the accounting section 310 computed. Since it is necessary to prevent an operator with malice altering accounting information here, as for accounting information, it is desirable to store in a secure field [in / in storing in a hard disk in the condition of having enciphered **** / a hard disk] (field which cannot be accessed in an operator's normal operation).

[0062] The communications department 313 consists of modem equipment connected to the communication line, and its control software, and transmits to the accounting information recorded on the accounting information storing section 312, and the host computer 600 which has installed an operator's operator ID in the accounting center of a music center in suitable timing through a communication line. Here, the time of reaching constant value with for example, the amount of accounting, the time of reaching on a fixed date, etc. can be considered to be suitable timing. Of course, it is good, though it connects with a host computer whenever an operator records on the record medium 650 of an acquisition application.

[0063] The recording rate Management Department 314 increments this recording rate, whenever the Records Department 309 has memorized the recording rate which recorded the same superdistribution contents 10 on the

record medium 650 of an acquisition application and the Records Department 309 records the same superdistribution contents 10 on the record medium 650 of an acquisition application. Actuation of the digital data recording apparatus constituted as mentioned above is further explained to a detail using the flow chart which shows the contents of processing of drawing 12 henceforth.

[0064] If loaded with the record medium 200 of a selling application, a control section 303 will start processing of this flow chart, and will wait to perform actuation of a purport of wishing introduction of a related score in step S20. If such actuation is performed, in step S21, a takeoff connection 304 will read the playback control script 4 and the still picture data 5 from the added value field 2 of the record medium 200 of the selling application, and the dialogue screen shown in drawing 8 will be displayed on a display 302. Then, it waits to shift to step S22 and to perform purchase directions of the superdistribution contents 10 from an operator. When purchase directions are performed, it shifts to step S23 from step S22, and the container 6 which contains the being enciphered encryption header 7 in a takeoff connection 304 from the record medium 200 of a selling application is made to take out, although processing is ended when an operator performs cancellation actuation. Then, in step S24, the superdistribution header 9 is obtained by decrypting the encryption header 7 in the taken-out container 6. If the superdistribution header 9 is obtained, the count

on which the same superdistribution contents 10 were recorded in step S25 until now will be read from the recording rate Management Department 314. The count of digital output authorization is read from the superdistribution header 9 obtained by decode in step S26 with it. If the count of digital output authorization is read, it will set to step S27 and will judge whether the recording rate of until is equal to the count of digital output authorization. If equal, since the digital output of the superdistribution contents 10 beyond this cannot be permitted, processing is ended as it is. On the other hand, if an old recording rate is less than the count of digital output authorization, a control section 303 uses the decode key 13 in the superdistribution header 9 for the superdistribution contents decryption section 306 in step S28, and makes the encryption contents 8 in a container decrypt.

[0065] When decode is performed, a control section 303 makes the proper information takeoff connection 307 acquire the identification information of a medium proper from the record medium 650 of an acquisition application in step S29, and makes the superdistribution contents re-encryption section 308 encipher data by making acquired identification information into a cryptographic key. Then, it shifts to step S30 and the data enciphered by the Records Department 309 are made to record on the record medium 650 of an acquisition application.

[0066] When record by the Records Department 309 is completed, a control section 303 makes the accounting section 310 compute the amount of accounting based on the acquisition price information in the purchase condition 12, and is made to store in the accounting information storing section 312 as accounting information in step S31. If waiting and such timing come that suitable timing to transmit accounting information in step S32 comes after making accounting information store, in step S33, a control section 303 will make the communications department 313 take out Operator ID with the accounting information recorded on the accounting information storing section 312, will make it transmit to the host computer 600 in an accounting center, and will end processing.

[0067] According to this operation gestalt, the consumer who acquired the record medium 200 of a selling application as mentioned above Only when it has agreed on the onerous purchase of these superdistribution contents 10, the superdistribution contents 10 currently recorded on the record medium 200 of a selling application are recorded on the record medium 650 of an acquisition application. Since only the accounting information which shows the frame of the countervalue to this record action is made to transmit to an accounting pin center,large through a communication line, there is no need of making the superdistribution contents 10 transmitting to a communication line. Therefore,

since the communication link tariff which a consumer should pay can be managed with a small sum even if it is in the condition which the transmission speed of a communication line cannot say that it is late and the infrastructure of an electronic music distribution is fixed, dealing of the superdistribution contents 10 is cheaply realizable.

[0068] Above, explanation of the 3rd operation gestalt is finished, and the 4th operation gestalt is explained continuously.

(The 4th operation gestalt) The 4th operation gestalt is related with the digital data regenerative apparatus which performs onerous playback of superdistribution contents. although the point which decrypt this digital data regenerative apparatus 400 as it is , without recording the data of the superdistribution format in the record medium 200 of a selling application on other record media , and be reproduce differ from the digital data recording apparatus 300 explained with the 3rd operation gestalt greatly , the digital data regenerative apparatus 400 have the download function [in / like the digital data recording apparatus 300 / an electronic music distribution] in the 3rd operation gestalt , i.e. , the function receive contents from the Internet for counter value . Therefore, the digital data regenerative apparatus contains many digital data recording devices 300 and common components. Drawing 13 is drawing showing the configuration of the digital data regenerative apparatus concerning

the 4th operation gestalt. Among the components of the digital data regenerative apparatus in drawing 13 , the digital data recording apparatus 300 and the reference mark same about a common component as the digital data recording apparatus 300 are attached, and explanation is omitted. on the other hand, what attached the No. 400 reference mark among the components of a digital data regenerative apparatus (the playback section 401, count Management Department 402 of playback) is a component peculiar to the digital data regenerative apparatus 400 which the digital data recording apparatus 300 does not possess, and explains these components henceforth.

[0069] The playback section 401 in drawing 13 reproduces the superdistribution contents 10 decrypted by the superdistribution contents decryption section 306. Moreover, initiation of playback of the superdistribution contents 10 tells that to the accounting section 310. Suitable accounting is made, when the playback section 401 transmits playback initiation to the accounting section 310 and playback of the superdistribution contents 10 is performed with the 4th operation gestalt.

[0070] The count Management Department 402 of playback increments this count of playback, whenever the playback section 401 has memorized the count of playback which reproduced the same superdistribution contents 10 and reproduces the superdistribution contents 10 with the same playback section

401. Actuation of the digital data regenerative apparatus constituted as mentioned above is further explained to a detail using the flow chart which shows the contents of processing of drawing 14 henceforth.

[0071] In this flow chart, it is the processing as the flow chart which shows the contents of processing of drawing 12 that the step from step S28 and step S31 to step S33 is the same from step S20 to step S24. On the other hand, since it is processing that step S41 to the step S46 is peculiar to the 4th operation gestalt, only these steps are explained. In step S24, if the encryption header 7 in the taken-out container 6 is decrypted and the superdistribution header 9 is obtained, in step S41, the control section 303 of a digital data regenerative apparatus will read the count by which the same superdistribution contents 10 were reproduced until now from the count Management Department 402 of playback. With it, the count of playback authorization is read from the superdistribution header 9. Since playback of the superdistribution contents 10 beyond this cannot be permitted if the count of playback authorization is read, and a control section 303 judges whether the old count of playback is less than the count of playback authorization and it is equal in step S42, processing is ended as it is.

[0072] If the old count of playback is less than the count of playback authorization, current time will be read in step S43, and a control section 303 will read playback authorization time amount and a playback authorization date from

the superdistribution header 9 in step S44. If these are read, it will judge whether in step S45, current time has already passed playback authorization time amount and a playback authorization date. If it has not passed, it shifts to step S28 from step S45, the decode key 13 in the superdistribution header 9 is used for the superdistribution contents decryption section 306, and the encryption contents 8 in a container are made to decrypt, although processing will be ended if it has passed. Then, in step S46, the playback section 401 is controlled to reproduce the superdistribution contents 10.

[0073] Since the purport which playback started at the time of playback initiation of the superdistribution contents 10 is transmitted to the accounting section 310 as mentioned above according to this operation gestalt, whenever the superdistribution contents 10 are reproduced, a concert company can acquire a profit. In addition, the digital data recording device which made the acquisition function of the superdistribution contents 10 in the 3rd operation gestalt and the regenerative function of the superdistribution contents 10 unify may be constituted.

[0074] Above, explanation of the 4th operation gestalt is finished. Next, the 5th operation gestalt is explained.

(The 5th operation gestalt) Although it assumed that a music content was distributed using a record medium with the 1st operation gestalt - 4th operation

gestalt, it assumes that a music content is distributed in broadcast waves, such as not only a record medium but the Internet, satellite broadcasting service, and a cable TV, with the 5th operation gestalt. Drawing 15 is drawing showing the distribution gestalt of the music content in the 5th operation gestalt. In this Fig., the music content which contents packaging equipment 700 created is drawing showing being distributed through DVD-Audio701, CD702, the Internet 703, a cable TV 704, and a communication satellite 705. On the other hand, in this Fig., all, the contents regenerative apparatus 801 - the contents regenerative apparatus 809 are regenerative apparatus which reproduce a music content, and although they are exclusively for the regenerative apparatus 801 of the high-class machine only for music content playbacks, and music content playback, they have the regenerative apparatus 802 and 803 of a low-grade machine, the regenerative apparatus 804 and 805 of the pocket mold only for music content playbacks, the regenerative apparatus 806 and 807 that made the general-purpose personal computer equip with the hardware of dedication, the regenerative apparatus 808 of the set top box mold for reception of satellite broadcasting service or CATV, and 809 grades.

[0075] As mentioned above, there is a thing various type in the regenerative apparatus used as the distribution place of a music content. The public welfare device type regenerative apparatus 801 only for music content playbacks and

802 grades possess exclusive hardware, in order to cancel encryption. On the other hand, the regenerative apparatus 806 of a general-purpose personal computer mold and 807 grades cancel encryption by not providing such exclusive hardware but operating decode software on general-purpose hardware. From these things, a copyright protection feature has not fixed the general-purpose personal computer etc., and a copyright protection feature can say that a public welfare device type regenerative apparatus is maintenance ending. Moreover, a public welfare device has the high quality at the time of reproducing contents, and a general-purpose personal computer has the low quality at the time of reproducing contents. Therefore, as for the regenerative apparatus with the high playback quality of contents, the copyright protection feature is fixed, and it turns out that a copyright protection feature has not fixed the regenerative apparatus with the low playback quality of contents.

[0076] If the internal configuration of contents packaging equipment 700 and regenerative apparatus 801-809 is described functionally, it will become like drawing 16 . Drawing 16 is drawing showing the internal configuration of the contents packaging equipment 700 in the 5th operation gestalt, and the contents regenerative apparatus 801-809. In this Fig., contents packaging equipment 700 contains the contents coding section 706, contents quality and the code conversion table storing section 707, the contents encryption section 708, and

the contents packing section 709.

[0077] The contents coding section 706 obtains two or more contents from which the quality at the time of playback differs by encoding the candidate for distribution by different method. By this coding, the contents 710 for sale and the contents 711 for sample offer reproduced in the low quality in which quality is inferior to the contents for sale shall be obtained. Contents quality and the code conversion table storing section 707 store the 2nd conversion table which made the group the 1st conversion table matched with the rank which should be given to the contents of the quantifying bit number at the time of carrying out the sign of the contents and a sampling frequency, and a this quantifying bit number and a sampling frequency, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank.

[0078] An example of the 1st conversion table is shown in drawing 17 (a). As shown in drawing 17 (a), it turns out that the quantifying bit number of 24 bits and the sampling frequency of 96kHz are matched with the rank 1 in the 1st conversion table, and the quantifying bit number of 16 bits and the sampling frequency of 22.05kHz are matched by the quantifying bit number of 16 bits, the sampling frequency of 44.1kHz, and the rank 3 at the rank 2. Thus, the more a quantifying bit number and a sampling frequency are high, the more it turns out that the rank estimator matched is high (it is here and the rank estimator means

that a rank is so high that there are few numeric values).

[0079] An example of the 2nd conversion table is shown in drawing 17 (b). As shown in drawing 17 (b), it turns out that the cryptographic key of 1024 bits and encryption algorithm called RSA are matched with the rank 1 in the 2nd conversion table, and the cryptographic key of 512 bits in a rank 2, the cryptographic key of 56 bits in encryption algorithm called RSA and a rank 3, and encryption algorithm called DES are matched. Since safety of RSA is higher than DES among such encryption algorithms, and safety is so high that the bit length of a cryptographic key is long, the more a rank estimator is high in this way, the more it turns out that the safety of the cryptographic key matched and encryption algorithm is high.

[0080] The contents encryption section 708 is enciphered using the cryptographic key and encryption algorithm according to the rank shown in the conversion table in the contents by which each contents were given to the opium poppy with a rank, and the rank according to the height of playback quality. For example, the contents 710 for sale obtained by coding of a package are the candidates for distribution, and when it has the quantization frequency which is 24 bits, and the sampling frequency of 96kHz, the contents encryption section 708 gives the rank estimator of "1" to the contents 710 for sale based on the 1st conversion table shown in drawing 17 (a). After giving a rank estimator, the

contents encryption section 708 generates a 1024-bit cryptographic key (session key) as a cryptographic key corresponding to a rank 1 with reference to the cryptographic key column in the 2nd conversion table. Then, with reference to the encryption algorithm column in the 2nd conversion table, the contents encryption section 708 enciphers the cryptographic key of the 1024-bit length concerned with a public-key-encryption algorithm (RSA), and attaches it to the contents for sale to which the above-mentioned scramble processing was performed.

[0081] On the other hand, the contents 711 for sample offer are the candidates for distribution, and when it has the quantization frequency which is 16 bits, and the sampling frequency of 44.1kHz, the contents encryption section 708 gives the rank estimator of "2" to the contents 710 for sale based on the 1st conversion table shown in drawing 17 (a). After giving a rank estimator, the contents encryption section 708 generates a 512-bit cryptographic key (session key) as a cryptographic key corresponding to a rank 2 with reference to the cryptographic key column in the 2nd conversion table. Then, with reference to the encryption algorithm column in the 2nd conversion table, the contents encryption section 708 enciphers the cryptographic key of the 512-bit length concerned with a public-key-encryption algorithm (RSA), and attaches it to the contents for sample offer to which the above-mentioned scramble processing was performed.

[0082] The contents packing section 709 packs up the contents 710 for sale and the contents 711 for sample offer which were enciphered by the contents encryption section 708, and obtains the package according to a distribution gestalt. When the distribution gestalten of a music content are the Internet, satellite broadcasting service, CATV, etc., the contents packing section 709 changes and outputs this package to a TCP packet and a transport packet. Moreover, when the distribution gestalten of a music content are record media, such as CD-ROM and DVD-ROM, the contents packing section 709 changes a package into the file of formats, such as a UDF format (universal disk formatting), and records it on CD-ROM and DVD-ROM. Thus, if a package is recorded, as shown in drawing 18 , the package containing two or more contents will be distributed to various regenerative apparatus. Drawing 18 is drawing showing the package obtained when the contents packing section 709 in the 7th operation gestalt packed up.

[0083] Then, the contents regenerative apparatus 801-809 are explained. As shown in drawing 15 , although the contents regenerative apparatus 801-809 have the respectively original gestalt, they are common at the point containing the hardware engine performance and the decode conversion table storing section 810 shown in drawing 16 , the hardware performance-evaluation section 811, the contents unpacking section 812, the contents decryption section 813,

the contents storing section 814, and the contents playback section 815.

[0084] The hardware engine performance and the decode conversion table storing section 810 store the conversion table which matched a rank estimator, and two or more decode keys and decode algorithms. Although the rank estimator in the 1st conversion table which contents quality and the code conversion table storing section 707 store here, and the 2nd conversion table had the value according to the height of the playback quality in contents, notice the rank estimator in the conversion table stored in the hardware engine performance and the decode conversion table storing section 810 about being used in order to evaluate the hardware engine performance which each of regenerative apparatus 801-808 has. With the hardware engine performance which each of regenerative apparatus 801-808 has In order that the hardware of a regenerative apparatus may decode encryption, provide exclusive hardware or no is shown. Moreover, when the copyright protection feature is fixed, it is the value which quantified the high level of the discharge capacity of the encryption. It is shown that the copyright protection feature is fixed, so that the rank estimator of the hardware engine performance is high, and it is shown that the copyright protection feature has not fixed, so that the rank estimator of the hardware engine performance is low. In addition, in this operation gestalt, the rank estimator for evaluation of the hardware engine performance is expressed

using the unit of rank estimators A, B, and C, is the order of A->B->C and makes the hardware engine performance high. Drawing 17 (c) is drawing showing the hardware engine performance and decode conversion table which the hardware engine performance and the decode conversion table storing section 810 store. Although the rank A in the conversion table of drawing 17 (c) shows that the copyright protection feature is fixed, the decode key of 1024 bits and a decryption algorithm called RSA are matched with this rank A. On the other hand, Ranks B and C are the rank estimators which should be given to the regenerative apparatus with which the copyright protection feature is not fixed as compared with the regenerative apparatus of Rank A. It turns out that the decode key of 56 bits, the decode key of 56 bits in a decryption algorithm called RSA and Rank C, and a decryption algorithm called DES are matched with rank estimator B.

[0085] The hardware performance-evaluation section 811 computes the rank estimator which shows the engine performance of the hardware concerned by evaluating the engine performance of the hardware of a regenerative apparatus by detecting the existence of possession of the exclusive hardware for decoding encryption of contents, and computing the memory scale which can be used for decode processing in hardware. If a package is distributed by contents packaging equipment 700, the contents unpacking section 812 will acquire this

package, and will extract the contents for sale, and the contents for sample offer from this package.

[0086] The contents decryption section 813 chooses the thing according to the rank estimator evaluated by the hardware performance-evaluation section 811 among two or more decode keys which can be set in the hardware engine performance and the decode conversion table storing section 810, and a decode algorithm. Only the contents of which encryption should be canceled with the decode key and decode algorithm which were chosen among the contents extracted by the contents unpacking section 812 with it are separated, and encryption of the separated contents is canceled.

[0087] When the contents regenerative apparatus 801 which is the high-class device of the public welfare device mentioned above here is an object, it explains how decode of the contents by the contents decryption section 813 is performed. Since this contents regenerative apparatus 801 has the hardware of the dedication for decoding encryption, the hardware engine performance will be estimated Rank A by the hardware performance-evaluation section 811. Moreover, since the 1024-bit decode key and the decode algorithm of RSA are matched with Rank A in the hardware engine performance and the decode conversion table storing section 810, the contents decryption section 813 chooses a 1024-bit decode key and the decode algorithm of RSA. On the other

hand, since the contents 710 for sale are enciphered as the 1024-bit encryption key using the encryption algorithm of RSA, the contents decryption section 813 separates only the contents 710 for sale among the contents which the contents unpacking section 812 extracted from the package. And in order to cancel public key encryption, decryption processing is performed using the decode key distributed beforehand.

[0088] Then, when the contents regenerative apparatus 806 of the general purpose personal SOKON pewter mold of which encryption is canceled by operating decode software on general-purpose hardware is an object, it explains how decode of the contents by the contents decryption section 813 is performed. Since only general-purpose hardware has this contents regenerative apparatus 806, the hardware engine performance will be estimated Rank C by the hardware performance-evaluation section 811. On the other hand, since the 56-bit decode key and the decode algorithm of DES are matched with Rank C in the hardware engine performance and the decode conversion table storing section 810, the contents decryption section 813 chooses a 56-bit decode key and the decode algorithm of DES. On the other hand, since the contents 711 for sample offer are enciphered as the 56-bit encryption key using the encryption algorithm of DES, the contents decryption section 813 separates only the contents 711 for sample offer among the contents which the contents unpacking

section 812 extracted from the package. On the other hand, since DES is a common key encryptosystem, it can decode contents by the cryptographic key used at the time of encryption. Therefore, the contents decryption section 813 takes out a cryptographic key from the package concerned, and performs decryption processing, using this as a decode key.

[0089] The contents storing section 814 stores the contents decoded by the contents decryption section 813. The contents playback section 815 reproduces the contents [finishing / decode] once stored in the contents storing means 723. Encryption processing of level which is different as mentioned above, respectively in the contents 710 for sale and the contents 711 for sample offer reproduced in quality lower than these contents 710 for sale according to this operation gestalt is performed. Since it was made to carry out packaging as a package, with the contents packing means 713 in a playback side When the contents according to the reproducibility ability of hardware come to be chosen and reproduced and a general-purpose type, high-class type difference is in the regenerative apparatus of the distribution place of a music content, the contents according to this will be reproduced. Therefore, without taking the playback environment of contents into consideration, the side which offers contents can provide coincidence with the contents from which quality differs, and can protect the copyright over contents safely.

[0090] Explanation of the 5th operation gestalt is finished above. Next, the 6th operation gestalt is explained.

(The 6th operation gestalt) By encoding the remaining part for distribution, the 6th operation gestalt obtains the contents 710 for sale, and is related with amelioration of the contents packaging equipment 700 of packing this up in a package while the contents coding section 706 obtains the contents 711 for sample offer by encoding the head part for distribution. Drawing 19 is drawing showing the contents packaging equipment 700 in the 6th operation gestalt, and the contents regenerative apparatus 801-809.

[0091] this operation gestalt -- setting -- a rank predetermined in the contents encryption section 708 to the contents for sample offer -- giving -- difference -- a higher rank is given to contents. Enciphering the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, the contents packing section 709 packs up said two or more enciphered contents, and generates a package. Drawing 20 is drawing showing the package obtained when the contents packing section 709 in the 7th operation gestalt packed up.

[0092] According to this operation gestalt, there is an advantage of the magnitude of the package at the time of contents packaging being reduced, consequently reduction of transmission capacity and a package being recorded,

for example, being able to perform capacity saving of record media, such as a hard disk and CD-ROM, as mentioned above. Although explained based on the above-mentioned operation gestalt, it showed as an example of a system which can expect the best effectiveness in the present condition. Modification implementation of this invention can be carried out in the range which does not deviate from the summary. As a gestalt of typical modification implementation, there are some which are shown in (a) - (f) below.

[0093] (a) With the 1st operation gestalt - 4th operation gestalt, the record medium 650 of an acquisition application may be transposed to hard disks other than an optical disk, semiconductor memory, etc., although explained as optical disks, such as DVD-RAM.

(b) When recording accounting information in the 3rd - the 4th operation gestalt, although explained considering the accounting information storing section 312 as a hard disk of a personal computer, it is possible for it not to be restricted to a hard disk and to transpose to record media, such as an IC card.

[0094] (c) Although the digital data recording device 500 was explained in the 1st - the 4th operation gestalt supposing consisting of personal computers and being used by domestic, it cannot be overemphasized that you may install in stores, such as the existing record store.

(d) In the 1st - the 4th operation gestalt, although the information which an

information provider offers was explained as a music content, of course, what does not restrict to this and a music content, image contents, text, or image contents, a music content and text combined may be used.

[0095] (e) In the 5th operation gestalt, although the contents 710 for sale and the contents 711 for sample offer shall be distributed, it is not restricted to this, and when distributing three or more contents using the contents which have still more gradual quality, it can apply.

(f) A machine program may realize the procedure (drawing 10 , drawing 12 , drawing 14) explained with reference to the flow chart with this operation gestalt in the 1st - the 6th operation gestalt, this may be recorded on a record medium, and you may make it the object of circulation and sale. Although there are an IC card, an optical disk, a floppy disk, etc. in such a record medium, use is presented with the machine program recorded on these by being installed in a general purpose computer. This general purpose computer performs the installed machine program serially, and realizes the function of the digital data recording apparatus shown in this operation gestalt, and a digital data regenerative apparatus.

[0096]

[Effect of the Invention] The record medium applied to this invention as explained above The 1st contents and the 2nd contents which the 1st contents

are different contents and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make the encryption in the 2nd contents cancel is included. Since the header enciphered with the 2nd cipher system which is a cipher system with which discharge of the encryption is performed is recorded only when the 2nd key information beforehand distributed to predetermined equipment is used The 1st contents are a famous artist's newly released pieces of music, and if it is the score with which the 2nd contents are related, the consumer who purchased these 1st contents can obtain the music content of this related score by canceling encryption of the 1st cipher system and the 2nd cipher system. Since discharge of this encryption should just load with this record medium the predetermined equipment with which the 2nd key information for making that encryption cancel is distributed beforehand, if the consumer has such predetermined equipment at the house, he does not need to apply a long time and does not need to download contents. Moreover, in order to purchase the 2nd contents, it is not necessary to go to the retail store of contents specially. Thus, a consumer can obtain simply the score relevant to a famous artist's newly released piece of music.

[0097] Moreover, since various distribution costs concerning circulation of a record medium are added up to this one record medium, a concert company can

set up the amount of accounting to the 2nd contents at a reasonable price, and a consumer can obtain the 2nd contents for a freight cost etc. cheaply. In order to defend the 2nd contents which should perform playback or acquisition for counter value from unjust playback and record here Although we are anxious about the time amount which discharge of the encryption takes turning into long duration when the algorithm of a processing load of public key use etc. is heavy, the 2nd contents must be enciphered with an algorithm with high safety and the 2nd contents have the data size of several megabytes Since the 2nd contents itself are enciphered with the 1st cipher system and a header is enciphered with the 2nd cipher system, the record medium concerning this invention can extract the part enciphered with the algorithm of public key use only to a header, when the 2nd cipher system is the algorithm of public key use.

[0098] Thus, the part enciphered with an algorithm with high safety is extracted only to a header, and since the 1st key information for canceling encryption of the 1st contents in it is stored, as compared with the case where the 2nd contents itself are enciphered with the algorithm of public key use, time amount until it cancels the encryption in the 2nd contents can be shortened. Since time amount after this directs acquisition and playback of superdistribution contents until it becomes acquisition and reproducible is short and it ends, the probability which those who wished the purchase of superdistribution contents are not

irritated for fun, and cancels purchase becomes low. Since it is thought that the time amount which this discharge takes becomes very shorter than the time amount which download of the music content in an electronic music distribution takes, an operator can appreciate immediately the superdistribution contents which wished acquisition or playback.

[0099] A ****** [that said predetermined equipment has the function to charge here, and said header permits playback of the 2nd contents, or record to other record media further], The use limit information which shows the count of an upper limit in the case of permitting playback or record to other record media, When record is permitted by playback or other record media of the 2nd contents, the accounting information which shows the tariff which record to the tariff or other record media which the playback which should be made to charge said predetermined equipment takes takes is included, and a peach is good.

[0100] Since according to this record medium it does not permit that the 2nd contents' being recorded on other record media, for example and the 2nd contents are reproduced to infinity but an upper limit can be set up, the duplicate of the 2nd contents can overflow and it can prevent that playback of the 2nd contents is performed frequently and the 2nd contents obsolete. A ****** [that said predetermined equipment has the function to charge here, and said header permits playback of the 2nd contents, or record to other record media further],

The authorization period information which shows the authorization period in the case of permitting record in playback or other record media, When record is permitted by playback or other record media of the 2nd contents, the accounting information which shows the tariff which record to the tariff or other record media which the playback which should be made to charge said predetermined equipment takes takes may be included.

[0101] Since, as for consent, only the period shown in that authorization period information can perform the duplicate or playback of the 2nd contents according to this record medium, premium-added value, such as seasonal limitation and period limitation, can be given to the 2nd contents. A storing means to store at least one or more contents which should be recorded on a record medium here, A selection means to choose the contents as superdistribution contents when what should charge record to the playback or other record media exists in said one or more contents, So that the playback about selected superdistribution contents or record to other record media may be prevented, while accounting is not performed A 1st encryption means to encipher superdistribution contents based on the 1st cipher system, A generation means to generate a superdistribution header including the key information of which encryption of superdistribution contents is made to cancel, The generated superdistribution header is enciphered based on the 2nd cipher system with safety higher than

said 1st cipher system. The digital data recording device characterized by having a 2nd encryption means to give superdistribution contents, and a record means to record on a record medium by using one or more contents as digital data if a superdistribution header is given may be used.

[0102] Since this will be chosen as superdistribution contents and this will be enciphered, if a thing to be payment [countervalue] is in record to those playback or other record media among one or more contents which should be recorded on the record medium of a selling application according to this digital data recording device, while accounting is not performed, the playback about superdistribution contents or record to other record media can be prevented.

[0103] Superdistribution contents are enciphered, and since the superdistribution header containing the accounting information which shows the countervalue to superdistribution contents, and the contents key of which the regenerative apparatus of superdistribution contents is made to cancel encryption of superdistribution contents when a countervalue is paid is given to superdistribution contents, whenever playback of superdistribution contents or record to other record media is performed, a concert company can acquire a profit.

[0104] If the record medium with which the charger stage which loads with either [at least] the 1st record medium or the 2nd record medium here, and the

charger stage were loaded is the 1st record medium The read-out means which reads superdistribution contents from the 1st record medium, and a presentation means to show an operator the countervalue to record to the 2nd record medium of superdistribution contents, A discharge means to cancel encryption of the superdistribution contents read from the 1st record medium when the actuation which a reception means to receive the actuation from an operator, and the reception means received is actuation of the purport of a countervalue on which it agrees for paying, If the accounting means charged to an operator and a charger stage are loaded with the 2nd record medium used as the archive destination of superdistribution contents when directions of the purport of a countervalue on which it agrees for paying are received from an operator A digital data recording device equipped with a record means to record on the 2nd record medium of an archive destination by using as digital data the superdistribution contents of which encryption was canceled may be used.

[0105] According to this digital data recording device, since the consumer who acquired the record medium records the superdistribution contents currently recorded on the record medium on the record medium of an acquisition application and performs accounting to this record action only when [of the countervalue of these superdistribution contents] it has agreed for paying, there is no need of making superdistribution contents transmitting to a circuit.

Therefore, since the communication link tariff which a consumer should pay can be managed with a small sum even if it is in the condition which the transmission speed of a circuit cannot say that it is late and the infrastructure of an electronic music distribution is fixed enough, dealing of superdistribution contents is cheaply realizable.

[0106] The charger stage which loads with a record medium here, and the read-out means which will read this if superdistribution contents are recorded on the record medium with which the charger stage was loaded, A presentation means to show an operator the countervalue to playback of superdistribution contents, A reception means to receive the actuation from an operator, and a discharge means to cancel encryption of superdistribution contents when the actuation which the reception means received is actuation of the purport of a countervalue on which it agrees for paying, When directions of the purport of a countervalue on which it agrees for paying are received from an operator, a digital data regenerative apparatus equipped with the accounting means charged to an operator and a playback means to reproduce the superdistribution contents of which encryption was canceled may be used.

[0107] Since it charges at the time of playback initiation of superdistribution contents, whenever superdistribution contents are reproduced according to this digital data regenerative apparatus, a concert company can acquire a profit. A

coding means to obtain two or more contents from which the quality at the time of playback differs by encoding the candidate for distribution by different method here, A rank means to rank each contents according to the height of playback quality, A conversion table storing means to store the conversion table which made the group two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, Contents packaging equipment equipped with a packing means to generate the package containing said two or more enciphered contents may be used.

[0108] According to this contents packaging equipment, encryption processing of level which is different, respectively in the contents for sale and the contents for sample offer reproduced in quality lower than these contents for sale is performed. With a contents packing means Since it was made to carry out packaging as a package, in a playback side When the contents according to the reproducibility ability of hardware come to be chosen and reproduced and various types, such as a general-purpose type and a high-class type, exist in the regenerative apparatus of the distribution place of a music content, the contents according to this will be reproduced. Therefore, without taking the playback

environment of contents into consideration, the side which offers contents can provide coincidence with the contents from which quality differs, and can protect the copyright over contents safely.

[0109] While obtaining the contents for sample offer by encoding the part for distribution here encoding the remaining part for distribution -- difference -- with a coding means to obtain contents a rank predetermined to the contents for sample offer -- giving -- difference -- with a rank means to give a higher rank to contents Two or more ranks, and the cryptographic key and cryptographic algorithm which should be used in order to encipher the contents of each rank are made into the group. In one group A predetermined rank is matched. For another side to construct A conversion table storing means to store the conversion table matched with the rank higher than the predetermined rank concerned, An encryption means to encipher the contents to which the rank was given using the cryptographic key and encryption algorithm according to the rank shown in the conversion table, Contents packaging equipment equipped with a packing means to generate the package containing said two or more enciphered contents may be used.

[0110] According to this contents packaging equipment, there is an advantage of the magnitude of the package at the time of carrying out packaging of the contents being reduced, consequently reduction of transmission capacity and a

package being recorded, for example, being able to perform capacity saving of record media, such as a hard disk and CD-ROM.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] (a) It is drawing showing the appearance of Enhanced-CD.

(b) It is drawing showing the physical structure of Enhanced-CD.

[Drawing 2] (a) It is drawing showing the appearance of DVD-AUDIO.

(b) It is drawing showing a functional format of DVD-AUDIO.

[Drawing 3] It is drawing showing the plastics case of the dedication which contained the record medium for sale.

[Drawing 4] It is drawing showing the DS of a container 6.

[Drawing 5] It is drawing showing an example of the purchase conditions 12.

[Drawing 6] It is drawing showing how the selling purpose contents 3 in this operation gestalt and the superdistribution contents 10 circulate.

[Drawing 7] (a) It is drawing showing the procedure in which superdistribution contents are bought from the record medium 200 for -(d) sale to the record medium 650 of an acquisition application.

[Drawing 8] It is drawing showing an example of the dialogue screen displayed on the display screen of a regenerative apparatus by the playback control script 4 and the still picture data 5.

[Drawing 9] It is drawing showing the configuration of the digital data recording device 100 concerning the 2nd operation gestalt.

[Drawing 10] It is the flow chart which shows the contents of processing of the digital data recording apparatus 100 of the 2nd operation gestalt.

[Drawing 11] It is drawing showing the internal configuration of the digital data recording device 300 of the 3rd operation gestalt.

[Drawing 12] It is the flow chart which shows the contents of processing of the digital data recording apparatus 300 of the 3rd operation gestalt.

[Drawing 13] It is drawing showing the internal configuration of the digital data regenerative apparatus 400 of the 4th operation gestalt.

[Drawing 14] It is the flow chart which shows the contents of processing of the digital data regenerative apparatus 400 of the 4th operation gestalt.

[Drawing 15] It is drawing showing the distribution gestalt of the music content in the 5th operation gestalt.

[Drawing 16] It is drawing showing the internal configuration of the contents packaging equipment 700 in the 5th operation gestalt, and the contents regenerative apparatus 801-809.

[Drawing 17] (a) It is drawing showing an example of the 1st conversion table.

(b) It is drawing showing an example of the 2nd conversion table.

(c) It is drawing showing an example of the hardware engine performance and a decode conversion table.

[Drawing 18] It is drawing showing the package obtained when the contents packing section 709 in the 5th operation gestalt packed up.

[Drawing 19] It is drawing showing the internal configuration of the contents packaging equipment 700 in the 6th operation gestalt, and the contents regenerative apparatus 801-809.

[Drawing 20] It is drawing showing the package obtained when the contents packing section 709 in the 6th operation gestalt packed up.

[Description of Notations]

1 Contents Field

2 Added Value Field

3 The Selling Purpose Contents

4 Playback Control Script

5 Still Picture Data

6 Container

7 Encryption Header

8 Encryption Contents

9 Superdistribution Header

10 Superdistribution Contents

11 Content ID

12 Purchase Conditions

13 Decode Key

100 Digital Data Recording Device

101 Input Section

102 Control Section

103 Encoding Section

104 Contents Storing Section

105 Takeoff Connection

106 Superdistribution Contents Encryption Section

107 Superdistribution Header Encryption Section

108 The Selling Purpose Contents Encryption Section

109 Records Department

110 Proper Information Takeoff Connection

200 Record Medium of Selling Application

300 Digital Data Recording Device

301 Input Section

302 Display

303 Control Section

304 Takeoff Connection

305 Superdistribution Header Decryption Section

306 Superdistribution Contents Decryption Section

307 Proper Information Takeoff Connection

308 Superdistribution Contents Re-Encryption Section

309 Records Department

310 Accounting Section

312 Accounting Information Storing Section

313 Communications Department

314 Recording Rate Management Department

400 Digital Data Regenerative Apparatus

401 Playback Section

402 Count Management Department of Playback

500 Communication Line

600 Host Computer

650 Record Medium of Acquisition Application

700 Contents Packaging Equipment

706 Contents Coding Section

707 Contents Quality and Code Conversion Table Storing Section

708 Contents Encryption Section

709 Contents Packing Section

710 Contents for Sale

711 Contents for Sample Offer

801-809 Contents regenerative apparatus

810 Hardware Engine Performance and Decode Conversion Table Storing Section

811 Hardware Performance-Evaluation Section

812 Contents Unpacking Section

813 Contents Decryption Section

814 Contents Storing Section

815 Contents Playback Section

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－196585
（P2000－196585A）
(43)公開日　平成12年７月14日(2000.7.14)

(51)Int.Cl.'		識別記号	FI			テーマコード'（参考）
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１	
Ｇ１１Ｂ	19/02	５０１	Ｇ１１Ｂ	19/02	５０１Ｊ	
	19/04	５０１		19/04	５０１Ｈ	
	20/10			20/10	Ｈ	

審査請求　未請求　請求項の数29　ＯＬ　（全 29 頁）

(21)出願番号　特願平11－287365

(22)出願日　平成11年10月７日(1999.10.7)

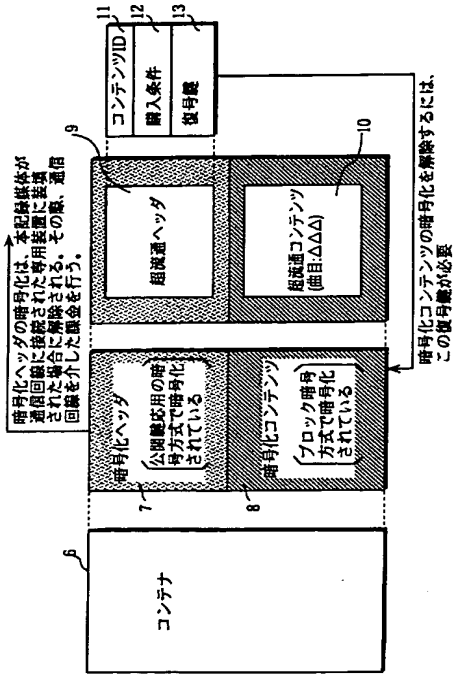
(31)優先権主張番号　特願平10－286177
(32)優先日　平成10年10月８日(1998.10.8)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－297159
(32)優先日　平成10年10月19日(1998.10.19)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－297142
(32)優先日　平成10年10月19日(1998.10.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　田川　健二
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　南　賢尚
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケージを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能

(57)【要約】
【課題】　電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で尚且つ手軽に販売することができる記録媒体を提供する。
【解決手段】　記録媒体には、販売目的のコンテンツが記録されており、それと共に、ブロック暗号方式に基づいて暗号化されている超流通コンテンツ１０が記録されている。この超流通コンテンツ１０に付与されている超流通ヘッダ９は、公開鍵応用の暗号化方式に基づいて暗号化されており、ブロック暗号方式の暗号化を解除させる復号鍵１３を含む。この公開鍵応用の暗号方式は、本記録媒体が通信回線に接続された装置３００、４００に装填された場合に、これらの装置により暗号化が解除される暗号方式であり、その暗号化の解除には、通信回線を介した課金が伴う。



1

【特許請求の範囲】

【請求項１】　第１コンテンツと、

第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、

第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されていることを特徴とする記録媒体。

【請求項２】　前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、

第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項１記載の記録媒体。

【請求項３】　前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、

第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項１記載の記録媒体。

【請求項４】　前記第１コンテンツは、

記録媒体固有の識別情報を用いて、暗号化されていることを特徴とする請求項１記載の記録媒体。

【請求項５】　コンテンツを含むデジタルデータを記録媒体に記録するデジタルデータ記録装置であって、

記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、

その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、

課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化手段と、

超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、

生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化手段と、

超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

2

【請求項６】　前記デジタルデータ記録装置は更に記録媒体固有の識別情報を記録媒体から取り出す取出手段と、

超流通コンテンツ以外のコンテンツについては、取出手段により取り出された識別情報を用いて暗号化する第３暗号化手段とを備えることを特徴とする請求項５記載のデジタルデータ記録装置。

【請求項７】　他の記録媒体への記録に課金が必要であり、課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されているコンテンツである超流通コンテンツを第１記録媒体から読み出して、第２記録媒体に記録するデジタルデータ記録装置であって、

第１記録媒体及び第２記録媒体の少なくとも一方を装填する装填手段と、

装填手段に装填された記録媒体が第１記録媒体であれば、超流通コンテンツを第１記録媒体から読み出す読出手段と、

超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示手段と、

操作者からの操作を受け付ける受付手段と、

受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、

装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

【請求項８】　前記デジタルデータ記録装置は更に装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、記録媒体固有の識別情報を、記録先となる第２記録媒体から取り出す取出手段と、

解除手段により暗号化が解除された超流通コンテンツを、取出手段が取り出した識別情報を暗号鍵として用いて、再度暗号化する再暗号化手段とを備え、

前記記録手段は、

再暗号化手段により再度暗号化された超流通コンテンツを記録先の第２記録媒体に記録することを特徴とする請求項７記載のデジタルデータ記録装置。

【請求項９】　その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されているコンテンツである超流通コンテンツを再生するデジタル

データ再生装置であって、
記録媒体を装填する装填手段と、
装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、
超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、
操作者からの操作を受け付ける受付手段と、
受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、
暗号化が解除された超流通コンテンツを再生する再生手段とを備えることを特徴とするデジタルデータ再生装置。

【請求項１０】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、
再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項１１】　前記対応表格納手段は、
前記高い品質で再生されるコンテンツには安全性が高い暗号が用いられるように、前記ランク情報と暗号鍵および暗号アルゴリズムを組にして格納していることを特徴とする請求項１０記載のコンテンツパッケージング装置。

【請求項１２】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、
試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納している対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項１３】　パッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムの組みとを対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項１４】　配布対象の一部分を符号化することにより得られた試供用コンテンツと、配布対象の残りの部分を符号化して、試供用コンテンツより安全性が高い暗号鍵及び暗号アルゴリズムにて暗号化することにより得られた差分コンテンツとを含むパッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
試供用コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを低いランク値と対応づけており、差分コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを高いランク値と対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に対応したものを選択すると共に、取得したパッケージから、試供用コンテンツ及び差分コンテンツの何れか一方を取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項１５】　所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化された試供用コンテンツと、
試供用コンテンツより高い品質で再生され、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化された販売用コンテンツとが記録されていることを特徴とす

る記録媒体。

【請求項１６】　配布対象の一部分を符号化した後、所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化することにより得られた試供用コンテンツと、
配布対象の残りの部分を符号化した後、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化することにより差分コンテンツとが記録されていることを特徴とする記録媒体。

【請求項１７】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置と、パッケージからコンテンツを取り出して再生するコンテンツ再生装置とからなるシステムであって、
前記コンテンツパッケージング装置は、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、
再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納しており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納する第１対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備え、
前記コンテンツ再生装置は、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している第２対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするシステム。

【請求項１８】　コンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、読み取ることができる記録媒体であって、
その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステップと、
課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化ステップと、
超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、
生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１９】　第１記録媒体、及び、第２記録媒体の何れか一方を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、
課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されていている超流通コンテンツが記録された第１記録媒体が、装填部に装填されればこれを第１記録媒体から読み出す読出ステップと、
超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示ステップと、
操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、
装填部に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２０】　記録媒体を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、
その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されていてる超流通コンテンツが記録された記録媒体が装填部に装填されれば、超流通コンテンツを読み出す読出ステップと、
超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付け

た場合、操作者に対して課金を行う課金ステップと、
操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再生する再生ステップとからなる手順をコンピュータに行わせる再生プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２１】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータが読み取ることができる記録媒体であって、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、
再生品質の高低に応じて、各コンテンツをランク付けするランク付とけステップと、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２２】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータが読み取ることができる記録媒体であって、
配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップと、
試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付けステップと、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２３】　複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している格納部を有するコンピュータが読み取ることができる記録媒体であって、
コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、

それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２４】　記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、コンテンツを含むデジタルデータを記録媒体に記録する記録方法であって、
その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステップと、
課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化ステップと、
超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、
生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項２５】　前記記録方法は、第１記録媒体及び第２記録媒体の何れかを装填する装填部を有したコンピュータに適用され、第１記録媒体に記録された超流通コンテンツを含むデジタルデータを第２記録媒体に記録する記録方法であって、第２記録媒体への記録に課金が必要であり、課金が行われていない間に第２記録媒体に記録されることを防止するため暗号化されている超流通コンテンツが記録された第１記録媒体が装填部に装填されればこれを第１記録媒体から読み出す読出ステップと、
超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示ステップと、
操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

装填部に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項２６】　記録媒体を装填する装填部を有したコンピュータに適用され、記録媒体に記録されているデジタルデータを再生する再生方法であって、

装填部に装填された記録媒体に、その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されている超流通コンテンツが記録されていればこれを読み出す読出ステップと、

超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、

受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再する再生ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【請求項２７】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、

配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、

再生品質の高低に応じて、各コンテンツをランク付けするランク付とけステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項２８】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、

配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップと、

試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付とけステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項２９】　複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納部を有したコンピュータに適用され、パッケージからコンテンツを取り出して再生するコンテンツ再生方法であって、

コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、

それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、

対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された音楽著作物を初めとするコンテンツを記録した記録媒体、コンテンツを記録媒体に記録する装置、記録媒体に記録されているコンテンツを再生する装置、複数のコンテンツをパッケージングする装置、コンピュータ読み取り可能な記録媒体、記録方法、再生方法、パッケージング方法に関する。

【０００２】

【従来の技術】（第１従来技術）次世代の音楽著作物の販売形態がどうあるべきかが、大手音楽会社、音響機器メーカ、有識者の間で盛んに議論されている。現状の音楽著作物の販売形態とは、ポップス、ロック、クラシック等様々なジャンルの音楽著作物をCD、磁気テープ等の記録媒体に記録して販売するという形態であり、このように販売された記録媒体を購入して音楽著作物を鑑賞するというライフスタイルは世界中に浸透しているといえる。

【０００３】記録媒体を用いた販売形態に対抗する販売

形態として、多くの注目を集めているのは、電子音楽配信と呼ばれる販売形態である。電子音楽配信とは、音楽コンテンツ（コンテンツとは、デジタル化された著作物のことをいい、音楽コンテンツとは、特に、デジタル化された音楽著作物のことをいう）の有料配布を、近年、急速な普及を見せているインターネット上で行うものである。この電子音楽配信の特色は、音楽コンテンツの販売の申し出や、音楽コンテンツを購入した者に対しての課金が電子商取引（Electronic Commerce)に準じて行われる点である。即ち、この電子音楽配信において音楽会社は、自身が開設したホームページに様々なコンテンツを紹介しており、消費者は、各音楽会社のホームページをアクセスすることにより、様々なコンテンツを検索することができる。好みのコンテンツがあった場合、消費者はコンテンツの購入要求、操作者ID等を、この音楽会社に通知する。音楽会社は、予め操作者により通知されているクレジットカードの番号に対応する銀行口座に基づいて、コンテンツの購入代金の決済を行うことができる。このような決済後、消費者は、消費者が所有しているコンピュータにコンテンツをダウンロードし、自分の好みのコンテンツを入手することができる。

【０００４】このように電子音楽配信では、対話的な選択操作に応じてダウンロードを行うので、例えば、認知度が高い新譜のコンテンツの販売を行っているホームページにおいて、その新譜のコンテンツを作詞･作曲したアーティストの他の楽譜のコンテンツや、その新譜のコンテンツを歌う歌手の他の楽譜のコンテンツを紹介すれば、これら他の楽譜を消費者に売り込むことができる。即ち、あるアーティストの新譜を購入しようとする消費者は、そのアーティストの関連する楽譜に強い興味を示していることが統計的に明らかであり、電子音楽配信では、そのような関連する複数の楽譜の売り込みを効率的に行うことができるのである。

【０００５】（第２従来技術）第１従来技術で述べたように、音楽コンテンツの配布形態には、記録媒体を用いた販売形態、インターネット等の通信回線を用いた販売形態を初め様々なものがある。記録媒体と一言でいっても、記録媒体には、DVD-Audio、CD等の種類があり、これらは何れも異なった符号化方式により符号化された状態で音楽コンテンツを記録している。また、このような販売形態以外にも、衛星放送やケーブルTV等の放送波にて放送されることにより音楽コンテンツが配布される機会も多い。これらの配布は有償で行われるのが原則であるが、音楽コンテンツの知名度を高める目的で無償で試供される場合もある。

【０００６】記録媒体、放送波、通信回線というように、様々な形態で音楽著作物が配布される場合、たとえ配布すべき音楽著作物が一種類のみであっても、音楽著作物を配布する側は、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布せねばならない。ここで、異なる符号化方式で符号化せねばならないのは以下の理由による。即ち、既に各世帯に普及している再生装置、及び、これから普及しつつある再生装置には、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なるので、音楽コンテンツを同一の符号化方式にて一律に送信しても、著作権保護機構が全く活用されなかったり、再生装置が本来備えている再生能力が発揮できない恐れがあるからである。

【０００７】著作権保護機構が既に整備されている再生装置が存在するのなら、全ての形態で配布される音楽コンテンツを安全性が高い暗号鍵にて暗号化しておけば良いように思える。しかし音楽コンテンツには、試供用等、知名度向上の目的で配布されるものがあり、このような音楽コンテンツは低い品質で再生されれば良いので、そのように、低い品質でしか再生されない音楽コンテンツも一律に安全性が高い暗号鍵にて暗号化すれば、試供用に低い品質のコンテンツを再生するにも、そのような安全性が高い暗号鍵による暗号化を解かねばならない。これでは、安全性が高い暗号化を解除するだけの復号能力を有していない再生装置は、試供用のコンテンツを再生することが不可能となり、試供用コンテンツが再生される機会が少なくなってしまう。このように試供用コンテンツが再生される機会が少なくなれば、音楽コンテンツの試供にて、幅広く販売促進を図るという広告活動が本来の目標を失うことになる。以上の理由で、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布することが、必然的に行われていた。

【０００８】

【発明が解決しようとする課題】ところで第１従来技術において問題となるのは、電子音楽配信を実現するためのインフラストラクチャは、現状、充分整備されているとはいえず、消費者が電子音楽配信にて音楽コンテンツを入手するには、消費者に様々な負担が課されるという点である。ここで電子音楽配信の実現のために不可欠とされているインフラストラクチャのうち、代表的なものは、数メガバイトというデータサイズを有する音楽コンテンツを短時間で伝送することができる高速回線であるが、一般のインターネットユーザは、公衆回線を介してサーバをアクセスを行うことにより、インターネットを利用している。一般のインターネットユーザが利用する公衆回線の伝送速度は、高速回線の伝送速度を大きく下回ることが一般的である。このように一般のインターネットユーザが低速な公衆回線を介して、上述のように複数コンテンツを同時にダウンロードする場合、通信時間が長時間となるので、消費者は、多大な通信料金を通信会社に支払うことになる。極端な場合、コンテンツの購入に関し消費者が音楽会社に支払う料金よりも、通信料金のほうが高くなってしまうことが有り得る。このように、消費者に多大な料金が課されるのであれば、電子音

楽配信を利用しようとする消費者の意欲は消沈してしまう。この料金面の問題にも増して懸念されるのは、複数のコンテンツを送信する場合、公衆回線における転送に要する時間が極めて長くなるので、コンテンツの購入を希望した者を悪戯に苛立たせてしまう点である。このようにコンテンツの転送が長ければ、コンテンツの購入を希望した者は複数コンテンツのダウンロードの途中で、コンテンツの購入をキャンセルしてしまう可能性がある。

【０００９】かといって、記録媒体を用いた販売形態において、電子音楽配信と同様、関連する楽譜のコンテンツを売り込もうとする場合、記録媒体を収納したケースに同梱されるジャケットに、そのような関連する楽譜についてセールスポイントや、販売価格等を印刷しておき、関連楽譜の購入を推薦するという古典的な手法をとらざるを得ない。消費者は、このようなジャケットの印刷内容を見て、関連楽譜に興味を持った場合、その関連楽譜を購入するためコンテンツの小売り店に出向き、その関連楽譜が記録された記録媒体を購入することにより、関連楽譜を入手するのである。

【００１０】ここで小売り店に販売されている記録媒体の小売り価格には、記録媒体の製造や流通に係る様々なコストが計上されている。そのため、新譜が記録された記録媒体、関連楽譜が記録された記録媒体の双方を購入しようとする場合、それら記録媒体の製造や流通に係る様々なコストが計上された小売り価格を、2つのコンテンツのそれぞれについて支払う必要があるので、割高な料金を消費者は支払うことになる。

【００１１】また、現状の記録媒体を用いた販売形態において、消費者が関連楽譜を入手するには、消費者自身がわざわざ記録媒体の小売り店に出向かねばならないので、消費者は気軽に関連楽譜を購入することはできず、記録媒体の小売り店に出向くまでにそのような関連楽譜を購入しようとする意欲を失ってしまうこともある。また第２の従来技術において、音楽コンテンツの供給者は、配布形態に応じて、異なる符号化方式で符号化を行う必要があるので、符号化されるコンテンツの数が多ければ多い程、音楽コンテンツの供給者は、それら音楽コンテンツの管理及び配布に多大なストレスを感じるという点である。このようにストレスを感じるのは、符号化されるコンテンツの数が多くなれば、例えば、販売用のコンテンツと、試供用のコンテンツとを誤って配布する等、誤配布の確率も高くなるからである。このような誤配布が生じれば、販売用コンテンツが公共の場に流出することになり、それらの全てを回収せねば、音楽コンテンツの供給者は経済的に大打撃を被ることになる。

【００１２】本発明の第１の目的は、電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で

尚且つ手軽に販売することができる記録媒体を提供することである。本発明の第２の目的は、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なる場合であっても、これらに対する音楽コンテンツの配信を一律に行うことができるコンテンツ梱包装置を提供することである。

【００１３】

【課題を解決するための手段】上記第１の目的は、第１コンテンツと、第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されている記録媒体により達成される。

【００１４】第２の目的は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置により達成される。

【００１５】

【発明の実施の形態】本発明に係る記録媒体、再生装置、記録装置についての実施形態について説明する。尚、記録媒体、再生装置、記録装置を一つの実施形態で説明しようとすると説明が著しく煩雑になるので、上記の内容を第１実施形態から第６実施形態において個別に説明するものとする。

【００１６】（第１実施形態）第１実施形態では、音楽コンテンツの販売用途に用いられる記録媒体について説明する。音楽コンテンツの販売用途に用いられる記録媒体には、販売目的の音楽コンテンツが記録されており、この記録媒体が有償で譲渡されることにより、コンテンツの販売がなされる。このような販売用途の記録媒体には、2つのタイプがある。1つ目のタイプは、販売を目的とした音楽コンテンツをEnhanced-CDに記録したものである。Enhanced-CDとは、内周部が通常のCD(CD-DA)と同じ物理構造になっていて、外周部がCD-ROMと同じ物理構造になっておりCD、CD-ROMの両方の機能を兼備したディスクをいう。本Enhanced-CDの外観を図１（ａ）に示し、Enhanced-CDの物理構造を図１（ｂ）に示す。図１

（ａ）においてEnhanced-CDの内周部は、CD-DA部と呼ばれ、外周部は、CD-ROM部と呼ばれる。これら、CD-DA部と、CD-ROM部を機能的に考えると、CD-DA部は、音楽コンテンツ３が記録されているコンテンツ領域１であり、CD-ROM部は、本記録媒体の付加価値を高めるデータを記録した付加価値領域２である。この販売用記録媒体は、このコンテンツ領域１に記録された音楽コンテンツを販売する用途に用いられる。

【００１７】2つ目のタイプの販売用途の記録媒体は、販売目的の音楽コンテンツ３が記録されたDVD-AUDIOである。本DVD-AUDIOの外観を図２（ａ）に示し、その論理フォーマットを図２（ｂ）に示す。このDVD-AUDIOにはEnhanced-CDに示したCD-DA部と、CD-ROM部は存在しないのに対して、販売目的コンテンツ３、再生制御スクリプト４、静止画データ５、コンテナ６のそれぞれがパーソナルコンピュータでアクセス可能なファイルにて記録される。このようにファイルにて記録される点がEnhanced-CDと異なるが、機能的なデータ構造はEnhanced-CD同様であり、コンテンツ領域１と、付加価値領域２とからなる。また、DVD-AUDIOにおけるコンテンツ領域１に音楽コンテンツ３が記録され、付加価値領域２に本記録媒体の付加価値を高めるデータが記録されている点も、Enhanced-CDと同一である。Enhanced-CDとの違いは、Enhanced-CDのコンテンツ領域１には、販売目的コンテンツ３が何の暗号化も施されることなく、そのまま記録されているのに対して、DVD-AUDIOのコンテンツ領域１に記録されている販売目的の音楽コンテンツ３は、DVD-AUDIO固有の識別情報を用いて暗号化されている点である。

【００１８】これらの2つのタイプの販売用記録媒体は、通常のCDと同様、ジャケットや譜面カードを同梱した状態で、専用のプラスチックケースに収納される。図３は、販売用記録媒体を収納した専用のプラスチックケースを示す図である。ここでコンテンツ領域１に記録されているコンテンツの曲名を仮に曲名:○○○とすれば、販売用記録媒体のジャケットには、図３に示すように、曲名:○○○に関する写真が主として印刷されていることがわかる。

【００１９】以上の説明で、コンテンツ領域１、付加価値領域２はEnhanced-CD及びDVD-AUDIOの双方に存在することが明らかになった。続いて、付加価値領域２の記録内容について説明する。図１（ｂ）及び図２（ｂ）の右段に付加価値領域２の記録内容を示す。本図に示すように、付加価値領域２には、再生制御スクリプト４と、静止画データ５と、コンテナ６とが記録されていることがわかる。

【００２０】再生制御スクリプト４は、表示機能付きの装置に本販売用記録媒体が装填された場合、この装置の対話画面に表示させる内容を記述した情報であり、Macromedia Director形式、HTML形式で記述されている。ここでMacromedia Director形式とは、MS-Windows/MacOSの汎用オーサリングソフトの利用時にオーサリング手順の記述に用られる形式であり、HTML形式とは、インターネットブラウザの記述に頻用されている形式である。

【００２１】静止画データ５は、再生制御スクリプト４により再生される対話画面において、表示されるべき静止画像である。これらの再生制御スクリプト４、静止画データ５は、従来のEnhanced-CDにも存在するものであるが、本実施形態における静止画データ５及び再生制御スクリプト４は、従来のものと表示内容が異なる。即ち、従来の静止画データ５及び再生制御スクリプト４には、販売目的コンテンツ３の歌詞やプロモーション映像、ファンクラブや新譜案内等、販売目的コンテンツ３に関連する情報を表示させるものであるが、本実施形態における静止画データ５及び再生制御スクリプト４は、販売目的コンテンツ３とは異なる音楽コンテンツの購入及び再生を推薦する情報を上記装置に表示させる。

【００２２】例えば、販売目的コンテンツ３がある人気アーティストの新譜ならば、本実施形態における再生制御スクリプト４は、その人気アーティストの過去のヒット曲の購入及び再生を推薦している。これら再生制御スクリプト４にて購入及び再生が推薦されている音楽コンテンツが何であるかは、以降の説明で明らかにしてゆく。

【００２３】続いて、Enhanced-CD及びDVD-AUDIOの双方に含まれている付加価値領域２におけるコンテナ６について説明する。コンテナ６のデータ構造は、図４に示すものとなる。本図において、コンテナ６は、暗号化ヘッダ７と、暗号化コンテンツ８とからなり、暗号化ヘッダ７は超流通ヘッダ９を含んでいて、暗号化コンテンツ８は超流通コンテンツ１０を含んでいる。

【００２４】ここで"超流通"とは、筑波大学名誉教授森亮一氏らが唱えるデジタルコンテンツの流通形態である。超流通においてデジタルコンテンツは、予め定められた超流通ヘッダが付与された状態で流通する。この超流通ヘッダには、対価をうるべき権利者を示す対価の詳細に関する対価情報が記されており、消費者がこのデジタルコンテンツの利用を希望した場合、消費者が所有する機器がこれらの権利者情報･対価情報を解釈して使用記録を作成することにより、料金清算を行うのである。

【００２５】超流通ヘッダ９、超流通コンテンツ１０は、このような超流通を前提にした形式、即ち、超流通形式にて、コンテナ６内に収納されている。このように、コンテナ６内に暗号化された状態で収納されている超流通コンテンツ１０こそ、静止画データ５及び再生制御スクリプト４にて、購入及び再生が推薦されている音楽コンテンツである。

【００２６】上述したように超流通ヘッダ９には、権利者情報や対価情報等、超流通を安全に行うために重要な情報が示されているので、これの改竄等の不正行為を効率的に防止する必要がある。そのため、本実施形態にお

ける超流通ヘッダ９は、公開鍵暗号アルゴリズムを応用した暗号方式に基づいて暗号化されたデータ領域を含む（尚、超流通ヘッダ９全体が暗号化されていてもよい。以下の文では、超流通ヘッダ９全体が暗号化されているものとして説明を行う。）。一般に公開鍵暗号には、楕円暗号やRSA暗号(Rivest, Shamir, Adleman encryption)等の種類があることが広く知られている。これら公開鍵を用いて暗号化されたデータを復号するには、暗号化に用いた公開鍵とは異なる復号鍵を用いる必要があるので、公開鍵は、安全性が非常に高いといわれる。

【００２７】しかしながら、本実施形態において超流通ヘッダ９を暗号化する際に用いられる公開鍵応用の暗号方式は、単に公開鍵を用いるだけではなく、以下の点が改良されている。即ち、本実施形態における公開鍵応用の暗号方式では、超流通ヘッダ９内のデータ領域の暗号化を解くための復号鍵が所定の専用装置に予め配布されており、販売用記録媒体がこの専用装置に装填された際に、超流通ヘッダ９の暗号化が解除されるのである。本実施形態においてこの専用装置は、通信回線に接続されており、超流通ヘッダ９の暗号化が解除され、超流通コンテンツが再生されようとする際、又は、超流通コンテンツが他の記録媒体に記録される際、超流通コンテンツについての権利者が正当な対価を得るよう、当該専用装置は、通信回線を介した課金を行うのである。尚、様々な超流通コンテンツを販売用記録媒体に記録させようとする場合、超流通コンテンツのそれぞれの超流通ヘッダについて、異なる公開鍵を用いる。一方、専用装置は、それらの超流通ヘッダが異なる公開鍵を用いて暗号化されていても、共通の復号鍵を用いてこの超流通ヘッダを復号する。また本実施形態において専用装置は、超流通コンテンツを再生又は買い取る際の課金を通信回線を介して行うものとして説明するが、課金情報をICカード等の別の記録媒体に記録しておき、課金情報についての決済を別の装置で行っても良い。また、別の装置にてプリペイドカードによる課金を行ってもよい。

【００２８】超流通ヘッダ９の暗号化を解除するための復号鍵が専用装置に設けられており、販売用記録媒体上に存在しないので、悪意を持った者が販売用記録媒体を取得し、不正な機器を用いてこの超流通ヘッダ９の暗号化を解除しようとしたとしても、その暗号化が解除される確率は極めて低い。このように超流通コンテンツ１０の暗号化を不法に解除するのは極めて困難なので、超流通コンテンツ１０の商取引は、安全に行われる。

【００２９】尚、超流通コンテンツ１０の曲名を△△△とすると、図３に示すように、販売用記録媒体のジャケットには、△△△についての内容は一切印刷されていない。これは、一般の消費者が、「超流通コンテンツ１０は販売目的コンテンツ３を購入した者に無償で供与されるのではないか」と勘違いすることを防止するためである。

【００３０】続いて、超流通ヘッダ９の内容について、図４を参照しながら説明する。図４において最も右側の段は、超流通ヘッダ９の内容を示している。ここからも理解できるように超流通ヘッダ９は、コンテンツID１１、購入条件１２、復号鍵１３から構成されている。コンテンツID１１は、超流通コンテンツ１０を他のコンテンツと識別するための情報が記述されている。超流通コンテンツ１０は音楽コンテンツであるので、ISRC（International Standard Recording Code）等の識別情報がコンテンツID１１として記述される。ここでISRCとは、曲ごとにユニークに割り振られる固有のID情報であって、国コード（２つのASCII文字）、記録年（２桁の数字）、シリアル番号（５桁の数字）により構成される。

【００３１】購入条件１２は、コンテンツの購入条件に関する情報が記述されている。ここで、購入条件１２の一例を図５に示す。図５において「再生許可回数」欄には、再生可能な上限値が整数で記述される。「デジタル出力許可回数」とは、専用装置にデジタル出力端子が備られている場合、このデジタル出力端子を介したデジタル出力を許可するか否かを示し、許可する場合は、その出力回数が整数値で記述される。

【００３２】「再生許可時間」欄は、コンテンツの再生を許可する時間、すなわち再生できる時間が記述される。「再生許可期日」欄は、コンテンツの再生を許可する期日が記述される。再生が許可された期日が過ぎた場合、そのコンテンツの再生はできないことになる。「課金情報」欄は、超流通コンテンツ１０の買い取り時の価格、又は、再生時の価格を示す情報を含む。ここで、買い取り時の価格とは、コンテナ６内の超流通コンテンツ１０を他の記録媒体に記録する際に操作者に課される価格をいい、再生時の価格とは、従量課金、即ち、コンテナ６内の超流通コンテンツ１０の再生回数に応じた価格を表す。この課金情報は、電子商取引において、署名付きの購入申込書として扱われるものであり、これと、操作者IDとを専用装置が課金センタ内のホストコンピュータに送信することは、電子商取引において販売用記録媒体の所有者が超流通コンテンツ１０の購入を申し込むことを意味する。即ち、記録媒体を装填した専用装置は、操作者が超流通コンテンツ１０の再生又は買い取りに合意した場合、通信回線を介して、操作者IDと、この課金情報とを音楽会社の課金センタに送信する。一方、音楽会社の課金センタには、操作者の予めクレジットカード番号が登録されており、このカード番号に対応する銀行口座を予め知得しているので、操作者IDが送信されれば、その送信元の操作者のクレジットカード番号に対応する銀行口座から、課金情報に示される価格を引き落とすことにより、コンテンツの購入代金の決済を行う。

【００３３】復号鍵１３は、超流通コンテンツ１０を復号するための復号鍵である。超流通コンテンツ１０は、LPCM（Linear Pulse Code Modulation）形式、AAC（Adv

anced Audio Coding）形式、DTS（Digital Theater System）形式の音楽コンテンツであり、ブロック暗号方式で暗号化されている。ブロック暗号とは、コンテンツをある一定の長さ（ブロック長）毎に分割して、そのブロック単位で暗号化する方法のことをいい、DES（ブロック長は64bit固定）、RC5（ブロック長は可変）などがこれに相当する。このブロック暗号方式では、暗号化したキーと復号化するための鍵とが同一であるので、公開鍵程、安全性は高く無い。超流通コンテンツ１０の暗号化を解除するには復号鍵１３を入手せねばならないが、復号鍵１３は公開鍵応用の暗号方式で強固に暗号化された超流通ヘッダ９内に存在するので、安全性が高く、超流通コンテンツ１０の暗号化を不法に解除することは非常に困難である。結果として超流通コンテンツ１０は強固に保護されていることになる。

【００３４】このように、超流通コンテンツ１０の購入等に関する購入条件１２は、安全性が高い公開鍵にて暗号化されている超流通ヘッダ９内に含まれているので、課金情報の改竄や超流通ヘッダ９の復号は非常に困難となる。また、超流通コンテンツ１０を公開鍵にて暗号化するのではなく、超流通ヘッダ９のみが公開鍵にて暗号化されているので、超流通コンテンツ１０を得るには、超流通ヘッダ９の暗号化を解除して、復号鍵１３を取り出し、復号鍵１３を用いて超流通コンテンツ１０を解除すればよい。公開鍵応用方式で暗号化されている部分はヘッダ部分に限定されているので、暗号化を解除すべき箇所は短かく、超流通コンテンツ１０の買取や再生を指示してから、買取や再生が可能となる時間は短くて済むので、超流通コンテンツ１０を希望した者を悪戯に苛立たせることはない。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツ１０をすぐさま鑑賞することができる。

【００３５】続いて、販売目的コンテンツ、超流通ヘッダ及び超流通コンテンツについての管理情報について説明する。ここで販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていない。このように販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているため、CDプレーヤ、DVD-AUDIOプレーヤ（これは、後述するデジタルデータ再生装置４００を意味するものではない）により曲として認識され再生されるが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていないため、CDプレーヤ、DVD-AUDIOプレーヤにより曲として認識され再生されることはない。これはCDプレーヤ、DVD-AUDIOプレーヤが、超流通ヘッダ及び超流通コンテンツを、販売目的コンテンツ同様そのまま再生しようとすると、CDプレーヤ、DVD-AUDIOプレーヤは超流

通ヘッダ及び超流通コンテンツを復号することができず、無意味で耳障りな音声が出力されてしまうので、そのように超流通ヘッダ及び超流通コンテンツが販売目的コンテンツと同様に再生されることを避けるためである。このようなCD、DVD-AUDIOにおける管理情報に代えて、超流通ヘッダ及び超流通コンテンツには、自身を販売目的コンテンツと区別するための固有の管理情報にて管理されており、専用装置が超流通ヘッダ及び超流通コンテンツを読み出す場合、この固有の管理情報にて、超流通ヘッダ及び超流通コンテンツについての記録開始位置－記録終了位置は特定される。

【００３６】続いて、これら販売目的コンテンツ３及び超流通コンテンツ１０がどのようにして消費者に行き渡るか、超流通コンテンツ１０の超流通がどのように行われるかを図６を参照しながら明らかにしてゆく。図６は、本実施形態における販売目的コンテンツ３と、超流通コンテンツ１０とがどのように流通されるかを示す図である。図６において販売用記録媒体は、矢印y1に示すように音楽会社の直営工場に設置されたデジタルデータ記録装置１００が販売目的コンテンツ３と、再生制御スクリプト４と、静止画データ５と、コンテナ６と、を記録媒体２００に記録することにより、製造される。このようにして製造された販売用記録媒体２００は、通常のCD同様、矢印y2に示すようにトラックの運送等の流通経路を経て、小売り店の店頭で販売される。一般の消費者は、矢印y3に示すように販売されている販売用記録媒体２００を購入することができる。

【００３７】販売用記録媒体２００を購入した消費者は、販売目的コンテンツ３を通常のCD、DVD-AUDIO同様のスタイルで鑑賞することができる。即ち、本図の矢印y4に示すように、歩行中に携帯型の再生装置に再生させることにより、販売目的コンテンツ３を鑑賞することができる。ここで消費者の家庭内には、通信回線に接続された専用装置として、デジタルデータ記録装置３００やデジタルデータ再生装置４００が設置されているものとする。このうちデジタルデータ記録装置３００は、販売用記録媒体２００に記録されている超流通コンテンツ１０を有償で他の記録媒体に記録させるものであり、デジタルデータ再生装置４００は、販売用記録媒体２００に記録されている超流通コンテンツ１０を有償で再生させるものである。また販売用記録媒体２００に記録されている静止画データ５、再生制御スクリプト４は、図８に示す対話画面をこれらデジタルデータ記録装置３００、デジタルデータ再生装置に表示させるものである。図８は、再生制御スクリプト４及び静止画データ５にて再生装置の表示画面に表示される対話画面の一例を示す図である。図８における対話画面は、ライブ演奏の様子等、超流通コンテンツ１０を紹介する画像m1と、超流通コンテンツ１０の再生を推薦する旨のメッセージm2と、その再生に対しての賛同又は拒否を指定できるボタンm3、m1

3と、再生価格の額m4と、当該楽譜の購入を推薦する旨を記述した文字列m5と、その購入に対しての賛同又は拒否を指定できるボタンm6、m16と、その購入価格m7とを含んでおり、超流通コンテンツ１０の有償購入及び有償再生を推薦する内容になっていることがわかる。この対話画面にて、消費者がEnhanced-CDのコンテナ６内にどのような超流通コンテンツ１０が収録されているかを知得し、もしそれらに興味があれば、消費者は、デジタルデータ記録装置３００を用いてこの超流通コンテンツ１０を買い取ることができ、またデジタルデータ再生装置を用いてこの超流通コンテンツ１０を再生させることができる。超流通コンテンツ１０を買い取った際、超流通コンテンツ１０を再生させた際、デジタルデータ記録装置３００、デジタルデータ再生装置４００は、公衆回線を通じて必要な課金額を示す課金情報を送信する。送信された課金情報は、音楽センタの課金センタに設置してあるホストコンピュータ６００に伝送される。

【００３８】図７（ａ）～図７（ｄ）は、デジタルデータ記録装置３００を介して、販売用記録媒体２００から買取用途の記録媒体へのコピーを行う様子を示す図である。ここで買取用途の記録媒体としては、DVD-RAMを用いるものとする。図７（ａ）においてデジタルデータ記録装置３００に販売用記録媒体２００、買取用途の記録媒体６５０がセットされると、図７（ｂ）に示すように、デジタルデータ記録装置３００の操作者は、販売用記録媒体２００に記録されている著作物を買取用途の記録媒体６５０にコピーする。その後、買取用途の記録媒体６５０であるDVD-RAMを図７（ｃ）に示すようにイジェクトすれば、超流通コンテンツ１０の買い取りが完了する。このような買い取り後、DVD-RAMのカートリッジからDVD-RAMを取り出せば、DVD-RAMに記録されたコンテンツは、DVD-RAM対応型のDVD-Audioプレーヤを用いることにより再生される。ここで、DVD-RAM対応型のDVD-Audioプレーヤとは、DVD-Audioディスクのみならず、DVD-RAMの再生を行うことができるDVD-Audioプレーヤをいう。

【００３９】尚、本実施形態では、デジタルデータ記録装置３００は、超流通コンテンツをDVD-RAMに記録したが、メモリカードに記録してもよい。以上のような超流通において、超流通コンテンツ１０に対する課金額は、販売目的コンテンツ３の小売り価格と比較して、割安に設定することができる。何故なら、販売目的コンテンツ３の小売り価格には、Enhanced-CD及びDVD-AUDIOの運送費等、Enhanced-CD及びDVD-AUDIOの流通に係る様々な流通コストが計上されているのに対して、超流通コンテンツ１０の買い取りは、単に暗号化を解除するだけで良く、そのような流通コストが一切不要となるためである。

【００４０】以上のように本実施形態によれば、インターネット等に代表される電子データ配信のためのインフラストラクチャが整備されていない状況にあっても、関連する楽譜の売り込み等、電子音楽配信に近い形態で、対話的な音楽コンテンツの販売を行うことができる。尚、本実施形態では音楽を記録する記録媒体としてEnhanced-CDと、DVD-AUDIOとを用いたが、ハイブリッドタイプのDVD-AUDIO(DVD-AUDIO, DVD-ROMの機能を兼備したディスク)を用いてもよい。更に本実施形態では、販売用途の記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録するものとして説明を行ったが、無償配布される記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録してもよい。

【００４１】以上で、本発明の記録媒体に記録される第１実施形態、すなわち超流通形式のデータ構造の説明を終わる。

（第２実施形態）第２実施形態は、超流通形式のデータを記録媒体に記録するデジタルデータ記録装置１００に関する。図９に、第２実施形態に係わるデジタルデータ記録装置１００の構成を示す。第２実施形態のデジタルデータ記録装置１００は、汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインストールすることにより実現され、入力部１０１、制御部１０２、エンコード部１０３、コンテンツ格納部１０４、取り出し部１０５、超流通コンテンツ暗号化部１０６、超流通ヘッダ暗号化部１０７、販売目的コンテンツ暗号化部１０８、記録部１０９、固有情報取り出し部１１０を備え、超流通コンテンツを販売用途の記録媒体２００に記録する。以後、これらの構成要素についての説明を行う。

【００４２】なお、本実施形態では、以後、記録対象を音楽コンテンツであるとするが、これに限られるものではなく、映像データや文字データ、あるいはこれらの組み合わせのデータでもよい。また販売用途の記録媒体２００に記録されるべきデータとして、第１実施形態では、再生制御スクリプト４や静止画データ５を例示したが、これらが記録される手順については、本実施形態の主眼と異なるので説明を省略する。

【００４３】入力部１０１は、マウス、キーボード等のポインティングデバイスと接続されており、操作者の指示を受け付ける。ここで、操作者の指示とは、音楽コンテンツのエンコードの指示、あるいは、エンコードしたデータの取り出し要求などが挙げられる。制御部１０２は、入力部１０１の要求を解釈し、音楽コンテンツをエンコードすることを後述するエンコード部１０３へ指示する。あるいは、後述するコンテンツ格納部１０４に記録されている音楽コンテンツを取り出すことを、やはり後述する取り出し部１０５へ指示する。

【００４４】エンコード部１０３は、図示しないマスターテープ等に記録されている原音を例えばLPCM形式のデジタルデータに符号化し、AAC形式に圧縮して音楽コンテンツを生成する。その後第１実施形態に示したコンテ

ンツID１１を生成する。尚、デジタルデータ記録装置１００においてエンコード部１０３は必須ではない。何故なら、外部の業者に音楽コンテンツのエンコードを依頼し、エンコードされたデータをコンテンツ格納部１０４に記録する場合、エンコード部１０３は不必要となるからである。

【００４５】コンテンツ格納部１０４は、大容量のハードディスク装置であって、エンコード部１０３のエンコードにより得られた音楽コンテンツ、及び、第１実施形態に示したコンテンツID１１を格納する。取り出し部１０５は、制御部１０２からの指示に基づいて、エンコードにより得られた音楽コンテンツ並びに第１実施形態に示したコンテンツID１１をコンテンツ格納部１０４から取り出す。

【００４６】超流通コンテンツ暗号化部１０６は、第１実施形態で説明した復号鍵１３を用いて超流通コンテンツ１０を暗号化することにより、暗号化コンテンツ８を生成する。ここで、復号鍵１３は、本デジタルデータ記録装置１００の操作者が自由に設定することができる。超流通ヘッダ暗号化部１０７は、操作者により記述された超流通形式のデータの購入条件１２と、コンテンツID１１と、復号鍵１３とを結合させて超流通ヘッダ９を得て、これを暗号化することにより、暗号化ヘッダ７を得る。さらに、生成した暗号化ヘッダ７を超流通コンテンツ暗号化部１０６が暗号化した暗号化コンテンツ８に付与してコンテナ６を得る。

【００４７】固有情報取り出し部１１０は、販売用記録媒体２００がDVD-AUDIOであり、販売目的コンテンツ３を記録媒体固有の識別情報に基づいて暗号化する必要がある場合、販売用途の記録媒体２００の製造時にあらかじめ記録されている媒体固有の識別情報を取り出し、販売目的コンテンツ暗号化部１０８に出力する。尚、販売用記録媒体２００がEnhanced-CDであり、販売目的コンテンツ３を暗号化する必要がない場合、媒体固有の識別情報を取り出しは行わない。

【００４８】販売目的コンテンツ暗号化部１０８は、販売用記録媒体２００がDVD-AUDIOである場合、販売目的コンテンツ３を、記録媒体固有の識別情報に基づいて暗号化する。尚、販売用記録媒体２００がEnhanced-CDであり、販売目的コンテンツ３を暗号化する必要がない場合、販売目的コンテンツ暗号化部１０８は暗号化を行わない。尚、媒体固有の識別情報に基づいて暗号化する技術については、特開平５－２５７８１６号公報に開示されているので、ここでは詳しい説明は省略する。

【００４９】記録部１０９は、超流通ヘッダ暗号化部１０７により生成されたコンテナ６と、第二の暗号化部１０８で暗号化された販売目的コンテンツとを記録する。以上のように構成されたデジタルデータ記録装置に関して、以後図１０の処理内容を示すフローチャートを用いてその動作を説明する。なお、以下の動作に関しては、すでにエンコード部１０３により、原音のエンコードが完了していて、コンテンツ格納部１０４に複数の音楽コンテンツが得られているものとする。

【００５０】制御部１０２が起動されると、ステップＳ１において制御部１０２は、コンテンツ格納部１０４に格納している複数のコンテンツのうち、販売用途の記録媒体２００に記録すべきものの選択を待つ。コンテンツが選択されれば、ステップＳ２において制御部１０２は操作者からの音楽コンテンツを販売用途の記録媒体２００への記録指示を待つ。ここでの記録指示には、販売を目的として記録する旨の記録指示と、超流通を目的として記録する旨の記録指示とがある。記録指示があった場合、制御部１０２は、ステップＳ３においてそれが販売目的で記録する旨の記録指示か、それとも超流通形式での記録指示かを判定する。

【００５１】操作者が販売用途のコンテンツの記録指示を行った場合、ステップＳ３において、販売用途のコンテンツの記録指示がなされたと判定される。この場合、制御部１０２は、ステップＳ３からステップＳ８に移行し、ステップＳ８において販売用途の記録媒体２００のタイプがDVD-AUDIOであるか、Enhanced-CDであるかを判定する。Enhanced-CDなら、ステップＳ８からステップＳ６に移行して、取り出し部１０５に、選択された音楽コンテンツ及びコンテンツIDの取り出しを指示し、取り出された音楽コンテンツ及びコンテンツIDを販売用途の記録媒体２００に記録させる。一方、DVD-AUDIOなら、ステップＳ８からステップＳ９へと移行する。ステップＳ９において制御部１０２は、取り出し部１０５に、適切な音楽コンテンツ及びコンテンツIDの取り出しを指示すると共に、取り出された音楽コンテンツを販売目的コンテンツ暗号化部１０８に引き渡す。販売目的コンテンツ暗号化部１０８は、販売用途の記録媒体２００からの固有の識別情報の取り出しを、固有情報取り出し部１１０に指示し、これを受けた固有情報取り出し部１１０は、販売用途の記録媒体２００から固有の識別情報を取り出す。その後、ステップＳ９からステップＳ１０に移行して、販売目的コンテンツ暗号化部１０８は、固有情報取り出し部１１０により取り出された媒体固有の識別情報を暗号鍵として用いて暗号化を行なう。その後、ステップＳ１０からステップＳ６に移行し、記録部１０９は、販売目的コンテンツ暗号化部１０８で暗号化された販売目的コンテンツ及びコンテンツIDを販売用途の記録媒体２００に記録する。ステップＳ１からステップＳ６までの処理にて、販売目的コンテンツが販売用途の記録媒体２００が記録されたので、続いて、超流通コンテンツの記録指示がなされた場合の動作について説明する。

【００５２】記録指示が超流通形式であった場合は、制御部１０２は、取り出し部１０５に、選択された音楽コンテンツ及びコンテンツIDを取り出させて、コンテンツIDをヘッダ暗号化部１０７に出力させ、超流通コンテン

ツ暗号化部１０６に出力させる。超流通コンテンツ暗号化部１０６は、ステップＳ４において取り出されたコンテンツを暗号化することにより、暗号化コンテンツを生成する。更に制御部１０２は、ステップＳ５において超流通ヘッダ暗号化部１０７にコンテンツID１１と、購入条件１２と、復号鍵１３とを結合させ、暗号化を行わせることにより、暗号化ヘッダ７を生成させて、暗号化ヘッダ７を暗号化コンテンツ８に付与させることによりコンテナ６を生成する。その後、ステップＳ６に移行して、生成されたコンテナ６を販売用途の記録媒体２００に記録させる。記録媒体への記録が完了すると、ステップＳ７において、記録作業を終了するか否かを操作者に問い合わせ、もし終了するなら、本フローチャートにおける処理を終了する。続行するなら、ステップＳ７からステップＳ１に移行する。以上のように本実施形態によれば、販売用途の記録媒体２００に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツ１０として選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツ１０についての再生又は他の記録媒体への記録を防止することができる。

【００５３】超流通コンテンツ１０を暗号化し、超流通コンテンツ１０を再生又は買い取る場合に専用装置に課金を行わせる課金情報と、課金後に専用装置に超流通コンテンツ１０の暗号化を解除させる復号鍵１３とを含む超流通ヘッダ９を超流通コンテンツ１０に付与するので、超流通コンテンツ１０の再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【００５４】以上で、第２実施形態の説明を終わる。

（第３実施形態）次に、第３実施形態として、デジタルデータ記録装置３００についての説明を行う。超流通コンテンツ１０の買い取りという側面から、デジタルデータ記録装置３００の内部構成を機能的に記述すれば、デジタルデータ記録装置３００の内部構成は、図１１に示すものとなる。図１１は、第３実施形態のデジタルデータ記録装置３００の内部構成を示す図である。デジタルデータ記録装置３００は、本来電子音楽配信対応型のデジタルデータ記録装置であり、電子音楽配信におけるダウンロード機能、即ち、通信部３１３がコンテンツを有償でインターネットから受信して、買取用途の記録媒体６５０に記録する機能を有している。電子音楽配信対応型であるため、デジタルデータ記録装置３００は、インターネットの通信を行うための通信部や、通信回線において電子商取引を行った場合に、通信回線上で金銭の決済を行うための課金部を有している。

【００５５】図１１において、第３実施形態のデジタルデータ記録装置３００は、一般に汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインス

トールすることにより実現され、入力部３０１、表示部３０２、制御部３０３、取り出し部３０４、超流通ヘッダ復号化部３０５、超流通コンテンツ復号化部３０６、固有情報取り出し部３０７、超流通コンテンツ再暗号化部３０８、記録部３０９、課金部３１０、課金情報格納部３１２、通信部３１３、及び記録回数管理部３１４を備える。

【００５６】入力部３０１は、マウス、キーボード等のポインティングデバイスと接続されており、操作者からの曲の購入指示を受け付ける。『超流通』における曲の購入とは、『超流通形式のデータを別の記録媒体へ記録する』という行為が含まれる。ここで、デジタルデータ記録装置及びデジタルデータ再生装置にデジタル出力端子が備られている場合、これらのデジタル出力端子にデジタル出力を行わせるという行為も『曲の購入』に含まれる。何故なら、このようなデジタル出力端子に、別の記録媒体のドライブ装置を接続すれば、このドライブ装置を用いて超流通コンテンツ１０をこの記録媒体に記録させることができるからである。本実施形態において、デジタルデータ記録装置１００は、デジタル出力端子を有しており、ケーブルを介してDVD-RAMのドライブ装置を接続している。

【００５７】表示部３０２は、販売用途の記録媒体２００に記録されている再生制御スクリプト４、静止画データ５に基づいて対話画面を表示することにより、超流通コンテンツ１０の内容や、これを購入する際の対価の額等の情報を視覚的に提示する。制御部３０３は、入力部３０１を通じて入力された操作者の指示を解釈し、他の構成要素に指示を行う。あるいは、他の構成要素が出力した結果に応じて、次の処理の指示を行う。例えば、操作者から関連楽譜の購入指示があれば、後述する取り出し部３０４に、販売用途の記録媒体２００に記録されている超流通コンテンツ１０及び超流通ヘッダ９の取り出しを指示する。

【００５８】取り出し部３０４は、第２実施形態に示した販売用途の記録媒体２００に記録されているコンテナ６を取り出す。超流通ヘッダ復号化部３０５は、取り出し部３０４がコンテナ６を取り出すと、それに含まれるコンテナ６内の暗号化ヘッダ７に対して復号鍵１３を用いて復号化を行う。復号により超流通ヘッダ９が得られれば、これに含まれるコンテンツID１１、購入条件１２、復号鍵１３を参照することにより、超流通コンテンツ１０の購入条件を操作者に提示することができる。尚、超流通ヘッダを復号する際使用する復号鍵は、例えば、デジタルデータ記録装置３００にインストールされるアプリケーションプログラムにあらかじめ格納されているもの、あるいは、通信回線を介して、課金センタから配布されるものを用いる。

【００５９】超流通コンテンツ復号化部３０６は、超流通ヘッダ復号化部３０５が超流通ヘッダ９を復号化すれ

ば、これに含まれる復号鍵１３を用いて、暗号化コンテンツ８を復号化する。固有情報取り出し部３０７は、買取用途の記録媒体６５０から、媒体固有の識別情報を取り出す。ここで買取用途の記録媒体６５０は、DVD-RAMであるので、BCA（Burst Cutting Area）に書かれた情報を媒体固有の識別情報として用いる。この媒体固有の識別情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持った操作者がディスクの内容を複製したとしても、復号鍵のもとになる識別情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

【００６０】超流通コンテンツ再暗号化部３０８は、固有情報取り出し部３０７が取り出した買取用途の記録媒体６５０媒体固有の識別情報に基づき、超流通コンテンツ復号化部３０６が復号化した超流通コンテンツ１０を暗号化する。記録部３０９は、超流通コンテンツ再暗号化部３０８により暗号化された超流通コンテンツ１０を買取用途の記録媒体６５０に記録する。

【００６１】課金部３１０は、記録部３０９の処理の終了通知があると、超流通ヘッダ復号化部３０５が超流通ヘッダ９を復号することにより得られた購入条件１２から、課金情報を読み出して、その課金情報に基づいた課金額を算出し、課金情報に組み入れる。課金情報格納部３１２は、パーソナルコンピュータのハードディスクに相当し、課金部３１０が算出した課金額を含む課金情報を格納する。ここで、課金情報は、悪意を持った操作者が改竄することを防ぐ必要があるので、課金情報は、暗号化した状態でハードディスクに格納したり、ハードディスクにおけるセキュア領域（操作者の通常の操作では、アクセスできない領域）に格納することが望ましい。

【００６２】通信部３１３は、通信回線に接続されたモデム装置と、その制御ソフトウェアとで構成され、課金情報格納部３１２に記録された課金情報と、操作者の操作者IDとを適当なタイミングにおいて、音楽センタの課金センタに設置してあるホストコンピュータ６００に通信回線を介して送信する。ここで、適当なタイミングとは例えば、課金額がある一定値に達したときや、一定の期日に達したときなどが考えられる。勿論、操作者が買取用途の記録媒体６５０に記録するたびにホストコンピュータに接続するとしてもよい。

【００６３】記録回数管理部３１４は、記録部３０９が買取用途の記録媒体６５０に、同一超流通コンテンツ１０を記録した記録回数を記憶しており、記録部３０９が買取用途の記録媒体６５０に同一超流通コンテンツ１０を記録する度に、この記録回数をインクリメントする。以上のように構成されたデジタルデータ記録装置の動作について、以後図１２の処理内容を示すフローチャートを用いて更に詳細に説明する。

【００６４】制御部３０３は、販売用途の記録媒体２００が装填されると、本フローチャートの処理を開始し、ステップＳ２０において関連楽譜の紹介を希望する旨の操作が行われるのを待つ。そのような操作が行われれば、ステップＳ２１において取り出し部３０４がその販売用途の記録媒体２００の付加価値領域２から再生制御スクリプト４及び静止画データ５を読み出して、図８に示した対話画面を表示部３０２に表示させる。その後、ステップＳ２２に移行して、操作者から超流通コンテンツ１０の購入指示が行われるのを待つ。操作者がキャンセル操作を行った場合は、処理を終了するが、購入指示を行った場合、ステップＳ２２からステップＳ２３に移行して、取り出し部３０４に、販売用途の記録媒体２００から、暗号化されたままの暗号化ヘッダ７を含むコンテナ６を取り出させる。その後、ステップＳ２４において、取り出されたコンテナ６における暗号化ヘッダ７を復号化することにより、超流通ヘッダ９を得る。超流通ヘッダ９が得られると、ステップＳ２５において同一超流通コンテンツ１０がこれまで記録された回数を記録回数管理部３１４から読み出す。それと共に、ステップＳ２６において復号により得られた超流通ヘッダ９からデジタル出力許可回数を読み出す。デジタル出力許可回数が読み出されると、ステップＳ２７においてこれまでの記録回数がデジタル出力許可回数に等しいか否かを判定する。もし等しければ、これ以上の超流通コンテンツ１０のデジタル出力は許可し得ないので、そのまま処理を終了する。一方、これまでの記録回数がデジタル出力許可回数を下回るのなら、制御部３０３は、ステップＳ２８において超流通コンテンツ復号化部３０６に超流通ヘッダ９内の復号鍵１３を用いて、コンテナにおける暗号化コンテンツ８を復号化させる。

【００６５】復号が行われると、制御部３０３は、ステップＳ２９において固有情報取り出し部３０７に買取用途の記録媒体６５０から媒体固有の識別情報を取得させ、超流通コンテンツ再暗号化部３０８に、取得した識別情報を暗号鍵としてデータを暗号化させる。その後、ステップＳ３０に移行して、記録部３０９により暗号化されたデータを買取用途の記録媒体６５０に記録させる。

【００６６】記録部３０９による記録が完了すると、ステップＳ３１において制御部３０３は、課金部３１０に購入条件１２中の買い取り価格情報に基づいて、課金額を算出させ、課金情報格納部３１２に課金情報として格納させる。課金情報を格納させた後、ステップＳ３２において課金情報を伝送するのに適当なタイミングが到来するのを待ち、そのようなタイミングが到来すれば、ステップＳ３３において制御部３０３は通信部３１３に、課金情報格納部３１２に記録された課金情報と、操作者IDとを取り出させ、課金センタ内のホストコンピュータ

６００に送信させて、処理を終了する。

【００６７】以上のように本実施形態によれば、販売用途の記録媒体２００を取得した消費者が、この超流通コンテンツ１０の有償での購入に合意した場合のみ、販売用途の記録媒体２００に記録されている超流通コンテンツ１０を買取用途の記録媒体６５０に記録し、この記録行為に対する対価の額を示す課金情報のみを通信回線を介して課金センターに伝送させるので、超流通コンテンツ１０を通信回線に伝送させる必要は無い。故に、通信回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツ１０の売買を安価に実現することができる。

【００６８】以上で、第３実施形態の説明を終え、続いて第４実施形態の説明を行う。

（第４実施形態）第４実施形態は、超流通コンテンツの有償での再生を行うデジタルデータ再生装置に関する。本デジタルデータ再生装置４００は、販売用途の記録媒体２００中の超流通形式のデータを他の記録媒体に記録せずに、そのまま復号化して再生する点が第３実施形態で説明したデジタルデータ記録装置３００と大きく異なるが、デジタルデータ再生装置４００は、第３実施形態におけるデジタルデータ記録装置３００同様、電子音楽配信におけるダウンロード機能、即ち、コンテンツを有償でインターネットから受信する機能を有している。そのため、デジタルデータ再生装置は、デジタルデータ記録装置３００と共通の構成要素を多く含んでいる。図１３は、第４実施形態に係るデジタルデータ再生装置の構成を示す図である。図１３におけるデジタルデータ再生装置の構成要素のうち、デジタルデータ記録装置３００と共通の構成要素については、デジタルデータ記録装置３００と同一の参照符号を付して説明を省略する。一方、デジタルデータ再生装置の構成要素のうち４００番台の参照符号を付したもの（再生部４０１、再生回数管理部４０２）は、デジタルデータ記録装置３００が具備していない、デジタルデータ再生装置４００特有の構成要素であり、以降これらの構成要素について説明を行う。

【００６９】図１３における再生部４０１は、超流通コンテンツ復号化部３０６により復号化された超流通コンテンツ１０を再生する。また、超流通コンテンツ１０の再生を開始すると、その旨を課金部３１０に伝える。再生部４０１が再生開始を課金部３１０に伝達することにより、第４実施形態では、超流通コンテンツ１０の再生が行われた際、適切な課金がなされる。

【００７０】再生回数管理部４０２は、再生部４０１が同一の超流通コンテンツ１０を再生した再生回数を記憶しており、再生部４０１が同一の超流通コンテンツ１０を再生する度に、この再生回数をインクリメントする。以上のように構成されたデジタルデータ再生装置の動作

について、以後図１４の処理内容を示すフローチャートを用いて更に詳細に説明する。

【００７１】本フローチャートにおいてステップＳ２０からステップＳ２４まで、ステップＳ２８、ステップＳ３１からステップＳ３３までのステップは、図１２の処理内容を示すフローチャートと同一処理である。一方、ステップＳ４１からステップＳ４６までは、第４実施形態特有の処理なのでこれらのステップのみについて説明を行う。ステップＳ２４において、取り出されたコンテナ６における暗号化ヘッダ７が復号化され、超流通ヘッダ９を得ると、ステップＳ４１においてデジタルデータ再生装置の制御部３０３は、同一超流通コンテンツ１０がこれまで再生された回数を再生回数管理部４０２から読み出す。それと共に、超流通ヘッダ９から再生許可回数を読み出す。再生許可回数が読み出されると、ステップＳ４２において制御部３０３は、これまでの再生回数が再生許可回数を下回るか否かを判定し、もし等しければ、これ以上の超流通コンテンツ１０の再生は許可し得ないので、そのまま処理を終了する。

【００７２】これまでの再生回数が再生許可回数を下回るなら、ステップＳ４３において現在日時を読み出し、ステップＳ４４において制御部３０３は、再生許可時間及び再生許可期日を超流通ヘッダ９から読み出す。これらが読み出されると、ステップＳ４５において現在日時が既に再生許可時間及び再生許可期日を経過しているかを判定する。経過していれば処理を終了するが、経過していなければ、ステップＳ４５からステップＳ２８に移行して、超流通コンテンツ復号化部３０６に、超流通ヘッダ９内の復号鍵１３を用いて、コンテナにおける暗号化コンテンツ８を復号化させる。その後、ステップＳ４６において、超流通コンテンツ１０を再生するよう再生部４０１を制御する。

【００７３】以上のように本実施形態によれば、超流通コンテンツ１０の再生開始時に、再生が開始した旨を課金部３１０に伝達するので、超流通コンテンツ１０が再生される度に、音楽会社は収益を得ることができる。

尚、第３実施形態における超流通コンテンツ１０の買い取り機能と、超流通コンテンツ１０の再生機能とを一体化させたデジタルデータ記録装置を構成しても良い。

【００７４】以上で、第４実施形態の説明を終わる。次に第５実施形態の説明を行う。

（第５実施形態）第１実施形態～第４実施形態では、音楽コンテンツが記録媒体を用いて配布されることを想定していたが、第５実施形態では、記録媒体のみならず、インターネットや衛星放送やケーブルTV等の放送波にて音楽コンテンツが配布されることを想定している。図１５は、第５実施形態における音楽コンテンツの配布形態を示す図である。本図において、コンテンツパッケージング装置７００が作成した音楽コンテンツは、DVD-Audio７０１、CD７０２、インターネット７０３、ケーブルT

31

V７０４、通信衛星７０５を介して配布されていることを示す図である。一方本図において、コンテンツ再生装置８０１～コンテンツ再生装置８０９は何れも、音楽コンテンツを再生する再生装置であり、音楽コンテンツ再生専用の高級機の再生装置８０１、音楽コンテンツ再生専用であるが低級機の再生装置８０２、８０３、音楽コンテンツ再生専用の携帯型の再生装置８０４、８０５、汎用のパソコンに専用のハードウェアを装着させた再生装置８０６、８０７、衛星放送やCATVの受信用のセットトップボックス型の再生装置８０８、８０９等がある。

【００７５】音楽コンテンツの配布先となる再生装置には、上述したように様々なタイプのものがある。音楽コンテンツ再生専用の民生機器タイプの再生装置８０１、８０２等は、暗号化の解除を行うために専用ハードウェアを具備している。これに対して、汎用パソコン型の再生装置８０６、８０７等は、そのような専用ハードウェアを具備しておらず、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う。これらのことから、汎用パソコンなどは、著作権保護機構が未整備であり、民生機器タイプの再生装置は、著作権保護機構が整備済みであると言える。また、民生機器はコンテンツを再生する際の品質が高く、汎用パーソナルコンピュータはコンテンツを再生する際の品質が低い。故に、コンテンツの再生品質が高い再生装置は著作権保護機構が整備されており、コンテンツの再生品質が低い再生装置は著作権保護機構が未整備であることがわかる。

【００７６】コンテンツパッケージング装置７００及び再生装置８０１～８０９の内部構成を機能的に記述すると、図１６のようになる。図１６は、第５実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。本図において、コンテンツパッケージング装置７００は、コンテンツ符号化部７０６、コンテンツ品質・暗号対応表格納部７０７、コンテンツ暗号化部７０８、コンテンツ梱包部７０９を含む。

【００７７】コンテンツ符号化部７０６は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る。この符号化により、販売用コンテンツ７１０と、販売用コンテンツよりも品質の劣る低い品質で再生される試供用コンテンツ７１１とが得られるものとする。コンテンツ品質・暗号対応表格納部７０７は、コンテンツを符号する際の量子化ビット数及びサンプリング周波数と、この量子化ビット数及びサンプリング周波数のコンテンツに付与されるべきランクと対応づけた第１対応表と、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした第２対応表とを格納する。

【００７８】第１対応表の一例を図１７（ａ）に示す。図１７（ａ）に示すように、第１対応表におけるランク

32

1には、24bitといった量子化ビット数と、96KHzといったサンプリング周波数とが対応づけられており、ランク2には、16bitといった量子化ビット数と、44.1KHzといったサンプリング周波数、ランク3には、16bitといった量子化ビット数と、22.05KHzといったサンプリング周波数とが対応づけられていることがわかる。このように量子化ビット数及びサンプリング周波数が高ければ高い程、対応づけられているランク値は高いことがわかる（ここで、ランク値は、数値が少ない程、ランクが高いことを意味している）。

【００７９】第２対応表の一例を図１７（ｂ）に示す。図１７（ｂ）に示すように、第２対応表におけるランク1には、1024bitといった暗号鍵と、RSAといった暗号化アルゴリズムとが対応づけられており、ランク2には、512bitといった暗号鍵と、RSAといった暗号化アルゴリズム、ランク3には、56bitといった暗号鍵と、DESといった暗号化アルゴリズムとが対応づけられていることがわかる。これらの暗号化アルゴリズムのうち、RSAはDESより安全性が高く、暗号鍵のビット長が長い程、安全性は高いので、このようにランク値が高ければ高い程、対応づけられている暗号鍵及び暗号化アルゴリズムの安全性は高いことがわかる。

【００８０】コンテンツ暗号化部７０８は、再生品質の高低に応じて、各コンテンツをランク付けし、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する。例えば、パッケージの符号化により得られた販売用コンテンツ７１０が配布対象であり、24bitの量子化周波数と、96KHzのサンプリング周波数を有している場合、コンテンツ暗号化部７０８は、図１７（ａ）に示す第１対応表に基づいて、販売用コンテンツ７１０に"1"のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部７０８は、第２対応表における暗号鍵欄を参照して、ランク1に対応する暗号鍵として、1024bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部７０８は、第２対応表における暗号化アルゴリズム欄を参照して、当該1024bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて暗号化して、上記スクランブル処理が施された販売用コンテンツに添付する。

【００８１】一方、試供用コンテンツ７１１が配布対象であり、16bitの量子化周波数と、44.1KHzのサンプリング周波数を有している場合、コンテンツ暗号化部７０８は、図１７（ａ）に示す第１対応表に基づいて、販売用コンテンツ７１０に"2"のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部７０８は、第２対応表における暗号鍵欄を参照して、ランク2に対応する暗号鍵として、512bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部７０８は、第２対応表における暗号化アルゴリズム欄を参照して、当該512bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて

暗号化して、上記スクランブル処理が施された試供用コンテンツに添付する。

【００８２】コンテンツ梱包部７０９は、コンテンツ暗号化部７０８により暗号化された販売用コンテンツ７１０及び試供用コンテンツ７１１を梱包し、配布形態に応じたパッケージを得る。音楽コンテンツの配布形態がインターネット、衛星放送、CATV等である場合、コンテンツ梱包部７０９は、このパッケージをTCPパケット、トランスポートパケットに変換して出力する。また、音楽コンテンツの配布形態がCD-ROM、DVD-ROMなどの記録媒体である場合、コンテンツ梱包部７０９は、パッケージをUDF形式(ユニバーサルディスクフォーマット)等の形式のファイルに変換して、CD-ROM、DVD-ROMに記録する。このようにパッケージが記録されれば、図１８に示すように、複数のコンテンツを含むパッケージが様々な再生装置に配布されることになる。図１８は、第７実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【００８３】続いてコンテンツ再生装置８０１～８０９について説明する。図１５に示したように、コンテンツ再生装置８０１～８０９は、それぞれ独自の形態を有しているが、図１６に示すハードウェア性能･復号対応表格納部８１０、ハードウェア性能評価部８１１、コンテンツ開梱部８１２、コンテンツ復号化部８１３、コンテンツ格納部８１４、コンテンツ再生部８１５を含む点で共通している。

【００８４】ハードウェア性能･復号対応表格納部８１０は、複数のランク値と、復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している。ここでコンテンツ品質･暗号対応表格納部７０７が格納している第１対応表、第２対応表におけるランク値は、コンテンツにおける再生品質の高低に応じた値を有していたが、ハードウェア性能･復号対応表格納部８１０に格納されている対応表におけるランク値は、再生装置８０１～８０８のそれぞれが有するハードウェア性能を評価するために用いられることに注意されたい。再生装置８０１～８０８のそれぞれが有するハードウェア性能とは、再生装置のハードウェアが、暗号化を復号するために専用ハードウェアを具備しているか否を示し、また著作権保護機構が整備されている場合、その暗号化の解除能力の高さを定量化した値であり、ハードウェア性能のランク値が高い程、その著作権保護機構が整備されていることを示し、ハードウェア性能のランク値が低い程、その著作権保護機構が未整備であることを示す。尚、本実施形態において、ハードウェア性能の評価のためのランク値はランク値A,B,Cという単位を用いて表現し、A→B→Cの順で、ハードウェア性能は高いものとする。図１７（ｃ）は、ハードウェア性能･復号対応表格納部８１０が格納しているハードウェア性能･復号対応表を示す図である。図１７（ｃ）の対応表におけるランクAは、著作権保護機構

が整備されていることを示しているが、このランクAには、1024bitといった復号鍵と、RSAといった復号化アルゴリズムとが対応づけられている。一方、ランクB,Cは、ランクAの再生装置と比較して、著作権保護機構が整備されていない再生装置に付与されるべきランク値である。ランク値Bには、56bitといった復号鍵と、RSAといった復号化アルゴリズム、ランクCには、56bitといった復号鍵と、DESといった復号化アルゴリズムとが対応づけられていることがわかる。

【００８５】ハードウェア性能評価部８１１は、コンテンツの暗号化を復号するための専用ハードウェアの具備の有無を検出し、ハードウェアにおいて復号処理に用いることができるメモリ規模を算出することにより、再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する。コンテンツ開梱部８１２は、コンテンツパッケージング装置７００によりパッケージが配布されれば、このパッケージを取得して、このパッケージから販売用コンテンツ、及び試供用コンテンツを抽出する。

【００８６】コンテンツ復号化部８１３は、ハードウェア性能･復号対応表格納部８１０における複数の復号鍵及び復号アルゴリズムのうち、ハードウェア性能評価部８１１により評価されたランク値に応じたものを選択する。それと共に、コンテンツ開梱部８１２により抽出されたコンテンツのうち、選択された復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツのみを分離して、分離されたコンテンツの暗号化を解除する。

【００８７】ここで上述した民生機器の高級機器であるコンテンツ再生装置８０１が対象である場合、コンテンツ復号化部８１３によるコンテンツの復号がどのように行われるかについて説明する。このコンテンツ再生装置８０１は、暗号化を復号するための専用のハードウェアを有しているので、ハードウェア性能評価部８１１によりハードウェア性能がランクAと評価されることになる。またハードウェア性能･復号対応表格納部８１０においてランクAには、1024bitの復号鍵と、RSAの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部８１３は1024bitの復号鍵と、RSAの復号アルゴリズムとを選択する。一方、販売用コンテンツ７１０は1024bitの暗号化鍵と、RSAの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部８１３は、コンテンツ開梱部８１２がパッケージから抽出したコンテンツのうち、販売用コンテンツ７１０のみを分離する。そして、公開鍵暗号を解除するために予め配布されている復号鍵を用いて、復号化処理を行う。

【００８８】続いて、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う汎用パーソナルソコンピュータ型のコンテンツ再生装置８０６が対象である場合、コンテンツ復号化部８１３によるコンテンツの復号がどのように行われるかについて説

明する。このコンテンツ再生装置８０６は、汎用のハードウェアしか有していないので、ハードウェア性能評価部８１１によりハードウェア性能がランクCと評価されることになる。一方、ハードウェア性能･復号対応表格納部８１０においてランクCには、56bitの復号鍵と、DESの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部８１３は、56bitの復号鍵と、DESの復号アルゴリズムとを選択する。一方、試供用コンテンツ７１１は56bitの暗号化鍵と、DESの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部８１３は、コンテンツ開梱部８１２がパッケージから抽出したコンテンツのうち、試供用コンテンツ７１１のみを分離する。一方、DESは、共通鍵暗号なので、暗号化時に用いた暗号鍵により、コンテンツを復号することができる。よって、コンテンツ復号化部８１３は、当該パッケージから暗号鍵を取り出し、これを復号鍵として用いて、復号化処理を行う。

【００８９】コンテンツ格納部８１４は、コンテンツ復号化部８１３により復号されたコンテンツを格納する。コンテンツ再生部８１５は、いったんコンテンツ格納手段７２３に格納された復号済みのコンテンツを再生する。以上のように本実施形態によれば、販売用コンテンツ７１０と、この販売用コンテンツ７１０より低い品質にて再生される試供用コンテンツ７１１とをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段７１３によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等の差違がある場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【００９０】以上で第５実施形態の説明を終わる。次に第６実施形態の説明を行う。

（第６実施形態）第６実施形態は、コンテンツ符号化部７０６が、配布対象の先頭部分を符号化することにより試供用コンテンツ７１１を得ると共に、配布対象の残りの部分を符号化することにより販売用コンテンツ７１０を得て、これをパッケージに梱包するというコンテンツパッケージング装置７００の改良に関する。図１９は、第６実施形態における、コンテンツパッケージング装置７００と、コンテンツ再生装置８０１～８０９を示す図である。

【００９１】本実施形態においてコンテンツ暗号化部７０８は、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与する。ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化して、コンテンツ梱包部７０９は、前記暗号化された複数のコンテンツを梱包して、パッケージを生成する。図２０は、第７実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【００９２】以上のように本実施形態によれば、コンテンツパッケージング時のパッケージの大きさを縮小することができ、その結果、伝送容量の低減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。上記実施形態に基づいて説明してきたが、現状において最善の効果が期待できるシステム例として提示したに過ぎない。本発明はその要旨を逸脱しない範囲で変更実施することができる。代表的な変更実施の形態として、以下（ａ）～（ｆ）に示すものがある。

【００９３】（ａ）第１実施形態～第４実施形態では、買取用途の記録媒体６５０を、DVD-RAMなどの光ディスクとして説明を行なったが、光ディスク以外のハードディスク、半導体メモリなどに置き換えてもよい。

（ｂ）第３～第４実施形態において課金情報を記録するときには、課金情報格納部３１２をパソコンのハードディスクとして説明を行なったが、ハードディスクに限られるものではなく、ICカードなどの記録媒体に置きかえることが可能である。

【００９４】（ｃ）第１～第４実施形態においてデジタルデータ記録装置５００については、パソコンで構成され家庭内で用いられることを想定して説明を行なったが、既存のレコード店などの店舗に設置してもよいことはいうまでもない。

（ｄ）第１～第４実施形態において、情報提供者が提供する情報を音楽コンテンツとして説明したが、これに限るものでなく、音楽コンテンツ、映像コンテンツ、文字情報、あるいは、映像コンテンツと音楽コンテンツと文字情報の組み合わせたものなどでもよいことはもちろんである。

【００９５】（ｅ）第５実施形態において、販売用コンテンツ７１０と、試供用コンテンツ７１１とが配布されるものとしたが、これに限られるものではなく、さらに段階的な品質を有するコンテンツを用いて３つ以上のコンテンツを配信する場合においても適用することができる。

（ｆ）第１～第６実施形態において本実施形態でフローチャートを参照して説明した手順（図１０、図１２、図１４）等を機械語プログラムにより実現し、これを記録媒体に記録して流通･販売の対象にしても良い。このような記録媒体には、ICカードや光ディスク、フロッピーディスク等があるが、これらに記録された機械語プログラムは汎用コンピュータにインストールされることにより利用に供される。この汎用コンピュータは、インスト

ールした機械語プログラムを逐次実行して、本実施形態に示したデジタルデータ記録装置、デジタルデータ再生装置の機能を実現するのである。

【００９６】

【発明の効果】以上説明したように本発明に係る記録媒体は、第１コンテンツと、第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されているので、第１コンテンツが有名アーティストの新譜であり、第２コンテンツが関連する楽譜であれば、この第１コンテンツを購入した消費者は、第１暗号方式、第２暗号方式の暗号化を解除することにより、この関連する楽譜の音楽コンテンツを入手することができる。この暗号化の解除は、その暗号化を解除させるための第２鍵情報が予め配布されている所定の装置に、本記録媒体を装填すればよいので、消費者は、そのような所定の装置を自宅に有していれば、長時間をかけてコンテンツをダウンロードしなくてもよい。また、第２コンテンツを購入するためにわざわざコンテンツの小売り店に出向かなくてもよい。このように、消費者は、有名アーティストの新譜に関連する楽譜を簡易に入手することができる。

【００９７】また運送費等、記録媒体の流通に係る様々な流通コストは、この記録媒体一枚に対して計上されるので、音楽会社は第２コンテンツに対する課金額は割安に設定することができ、消費者は安価に第２コンテンツを入手することができる。ここで、有償で再生又は買い取りを行うべき第２コンテンツを不正な再生や記録から防御するためには、公開鍵利用のアルゴリズム等、処理負荷が重く、安全性が高いアルゴリズムで第２コンテンツを暗号化せねばならず、第２コンテンツが数メガバイトというデータサイズを有している場合は、その暗号化の解除に要する時間が長時間になることが懸念されるが、本発明に係る記録媒体は、第２コンテンツ自体が第１暗号方式にて暗号化され、ヘッダが第２暗号方式にて暗号化されるので、第２暗号方式が公開鍵利用のアルゴリズムである場合、公開鍵利用のアルゴリズムにて暗号化する箇所を、ヘッダのみに絞ることができる。

【００９８】このように安全性が高いアルゴリズムにて暗号化する箇所をヘッダのみに絞り、その中に第１コンテンツの暗号化を解除するための第１鍵情報を格納しておくので、第２コンテンツ自体を公開鍵利用のアルゴリズムで暗号化する場合と比較して、第２コンテンツにおける暗号化を解除するまでの時間を短くすることができる。これにより超流通コンテンツの買取や再生を指示してから、買取や再生が可能となるまでの時間は短くて済むので、超流通コンテンツの購入を希望した者を悪戯に苛立たせることはなく、購入をキャンセルする確率は低くなる。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツをすぐさま鑑賞することができる。

【００９９】ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいてもも良い。

【０１００】この記録媒体によれば、例えば第２コンテンツが他の記録媒体に記録されることや第２コンテンツが再生されることを無限に許可するのではなく、上限を設定できるので、第２コンテンツの複製が氾濫することや、第２コンテンツの再生が頻繁に行われて第２コンテンツが陳腐化するのを防止することができる。ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいてもよい。

【０１０１】この記録媒体によれば、その許可期間情報に示されている期間しか第２コンテンツの複製又は再生を許諾は行なえないので、季節限定、期間限定等のプレミア的な付加価値を第２コンテンツに与えることができる。ここで記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化手段と、超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化手段と、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置を用いてもよい。

【０１０２】このデジタルデータ記録装置によれば、販売用途の記録媒体に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツとして選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツについての再生又は他の記録媒体への記録を防止することができる。

【０１０３】超流通コンテンツを暗号化し、超流通コンテンツに対する対価を示す課金情報と、対価が支払われた場合に、超流通コンテンツの再生装置に超流通コンテンツの暗号化を解除させるコンテンツキーとを含む超流通ヘッダを超流通コンテンツに付与するので、超流通コンテンツの再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【０１０４】ここで第１記録媒体及び第２記録媒体の少なくとも一方を装填する装填手段と、装填手段に装填された記録媒体が第１記録媒体であれば、超流通コンテンツを第１記録媒体から読み出す読出手段と、超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とを備えるデジタルデータ記録装置を用いてもよい。

【０１０５】このデジタルデータ記録装置によれば、記録媒体を取得した消費者が、この超流通コンテンツの対価の支払いに合意した場合のみ、記録媒体に記録されている超流通コンテンツを買取用途の記録媒体に記録し、この記録行為に対しての課金を行うので、超流通コンテンツを回線に伝送させる必要は無い。故に、回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが充分整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツの売買を安価に実現することができる。

【０１０６】ここで記録媒体を装填する装填手段と、装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、暗号化が解除された超流通コンテンツを再生する再生手段とを備えるデジタルデータ再生装置を用いてもよい。

【０１０７】このデジタルデータ再生装置によれば、超流通コンテンツの再生開始時に、課金を行うので、超流通コンテンツが再生される度に、音楽会社は収益を得ることができる。ここで配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【０１０８】このコンテンツパッケージング装置によれば、販売用コンテンツと、この販売用コンテンツより低い品質にて再生される試供用コンテンツとをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等、様々なタイプが存在する場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【０１０９】ここで、配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納している対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【０１１０】このコンテンツパッケージング装置によれば、コンテンツをパッケージングする際のパッケージの大きさを縮小することができ、その結果、伝送容量の低

41

減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。

【図面の簡単な説明】

【図１】（ａ）Enhanced-CDの外観を示す図である。

（ｂ）Enhanced-CDの物理構造を示す図である。

【図２】（ａ）DVD-AUDIOの外観を示す図である。

（ｂ）DVD-AUDIOの機能的なフォーマットを示す図である。

【図３】販売用記録媒体を収納した専用のプラスチックケースを示す図である。

【図４】コンテナ６のデータ構造を示す図である。

【図５】購入条件１２の一例を示す図である。

【図６】本実施形態における販売目的コンテンツ３と、超流通コンテンツ１０とがどのように流通されるかを示す図である。

【図７】（ａ）～（ｄ）販売用記録媒体２００から買取用途の記録媒体６５０へと超流通コンテンツが買い取られる手順を示す図である。

【図８】再生制御スクリプト４及び静止画データ５にて再生装置の表示画面に表示される対話画面の一例を示す図である。

【図９】第２実施形態に係わるデジタルデータ記録装置１００の構成を示す図である。

【図１０】第２実施形態のデジタルデータ記録装置１００の処理内容を示すフローチャートである。

【図１１】第３実施形態のデジタルデータ記録装置３００の内部構成を示す図である。

【図１２】第３実施形態のデジタルデータ記録装置３００の処理内容を示すフローチャートである。

【図１３】第４実施形態のデジタルデータ再生装置４００の内部構成を示す図である。

【図１４】第４実施形態のデジタルデータ再生装置４００の処理内容を示すフローチャートである。

【図１５】第５実施形態における音楽コンテンツの配布形態を示す図である。

【図１６】第５実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。

【図１７】（ａ）第１対応表の一例を示す図である。

（ｂ）第２対応表の一例を示す図である。

（ｃ）ハードウェア性能･復号対応表の一例を示す図である。

【図１８】第５実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【図１９】第６実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。

【図２０】第６実施形態におけるコンテンツ梱包部７０

42

９が梱包を行うことにより得られたパッケージを示す図である。

【符号の説明】

１	コンテンツ領域
２	付加価値領域
３	販売目的コンテンツ
４	再生制御スクリプト
５	静止画データ
６	コンテナ
７	暗号化ヘッダ
８	暗号化コンテンツ
９	超流通ヘッダ
１０	超流通コンテンツ
１１	コンテンツID
１２	購入条件
１３	復号鍵
１００	デジタルデータ記録装置
１０１	入力部
１０２	制御部
１０３	エンコード部
１０４	コンテンツ格納部
１０５	取り出し部
１０６	超流通コンテンツ暗号化部
１０７	超流通ヘッダ暗号化部
１０８	販売目的コンテンツ暗号化部
１０９	記録部
１１０	固有情報取り出し部
２００	販売用途の記録媒体
３００	デジタルデータ記録装置
３０１	入力部
３０２	表示部
３０３	制御部
３０４	取り出し部
３０５	超流通ヘッダ復号化部
３０６	超流通コンテンツ復号化部
３０７	固有情報取り出し部
３０８	超流通コンテンツ再暗号化部
３０９	記録部
３１０	課金部
３１２	課金情報格納部
３１３	通信部
３１４	記録回数管理部
４００	デジタルデータ再生装置
４０１	再生部
４０２	再生回数管理部
５００	通信回線
６００	ホストコンピュータ
６５０	買取用途の記録媒体
７００	コンテンツパッケージング装置
７０６	コンテンツ符号化部

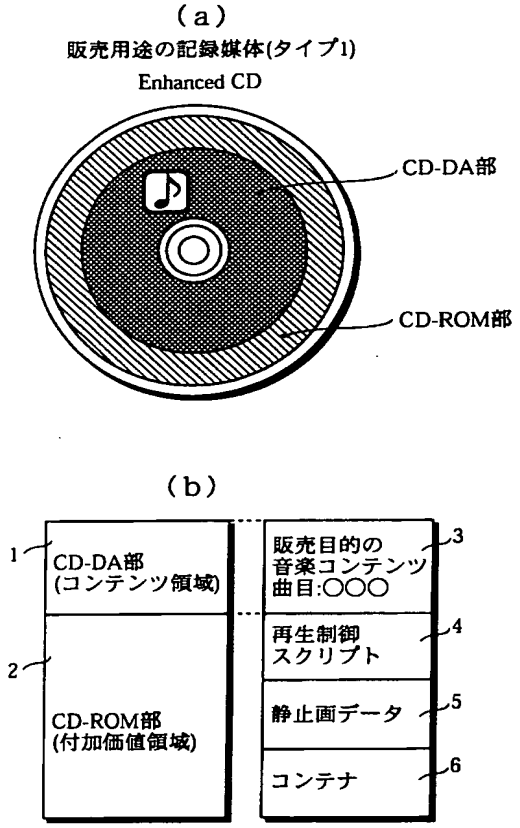
43

７０７　コンテンツ品質･暗号対応表格納部
７０８　コンテンツ暗号化部
７０９　コンテンツ梱包部
７１０　販売用コンテンツ
７１１　試供用コンテンツ
８０１～８０９　コンテンツ再生装置

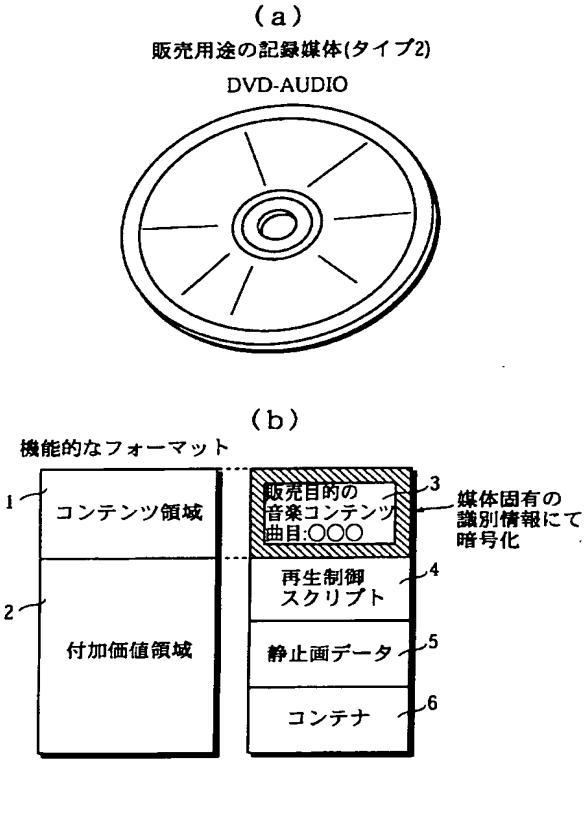
44

８１０　ハードウェア性能･復号対応表格納部
８１１　ハードウェア性能評価部
８１２　コンテンツ開梱部
８１３　コンテンツ復号化部
８１４　コンテンツ格納部
８１５　コンテンツ再生部

【図１】

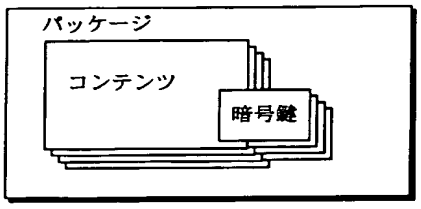


【図２】

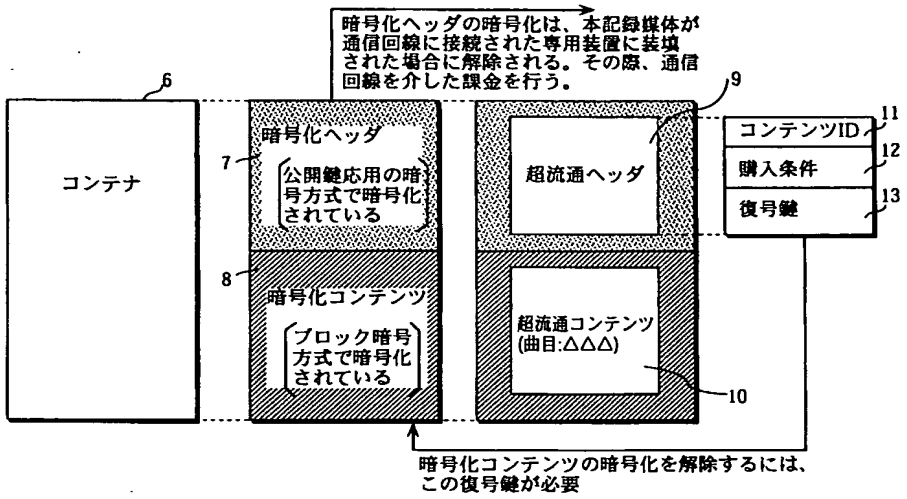


【図３】

【図１８】



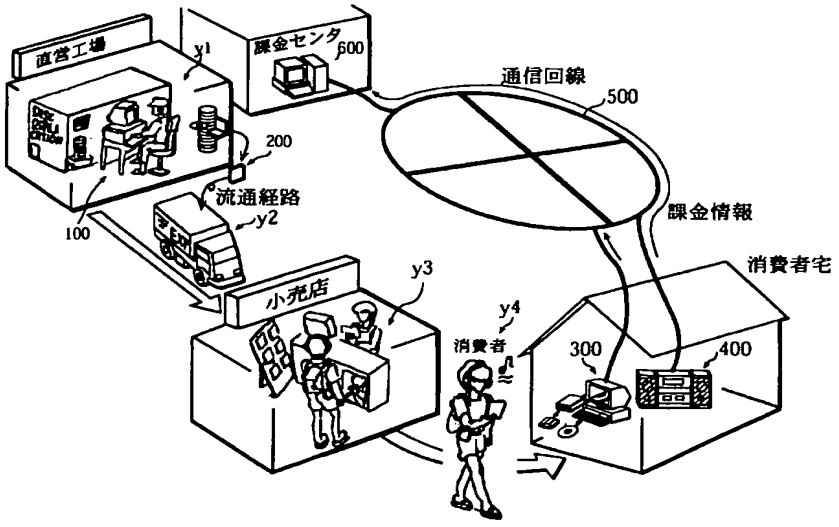
【図４】



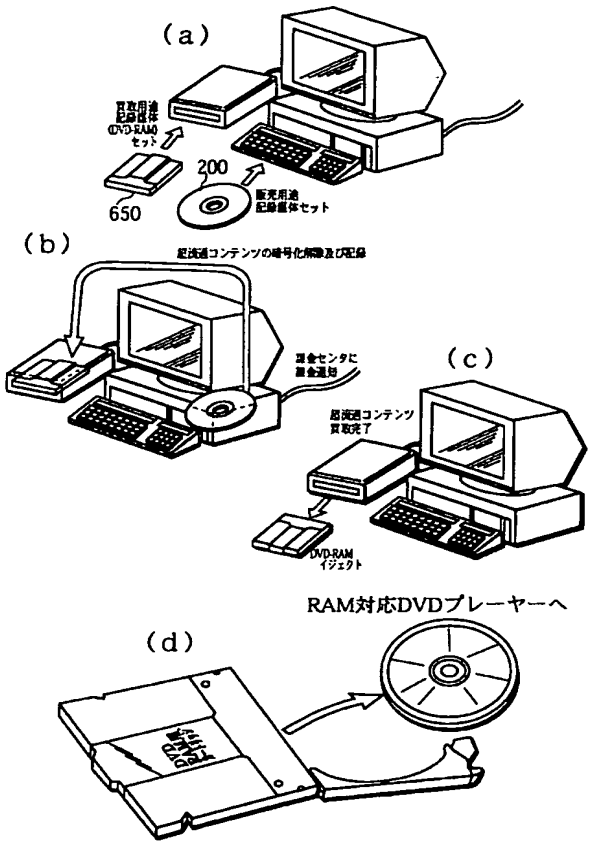
【図５】

名称	内容
再生許可回数	再生可能な回数を記述
ディジタル出力許可回数	ディジタル出力を許可するか否か。許可する場合はその回数を記述
再生許可時間	再生可能な時間を記述
再生許可期日	再生可能な期日を記述
課金情報	買取時の価格や再生回数による使用料金を記述

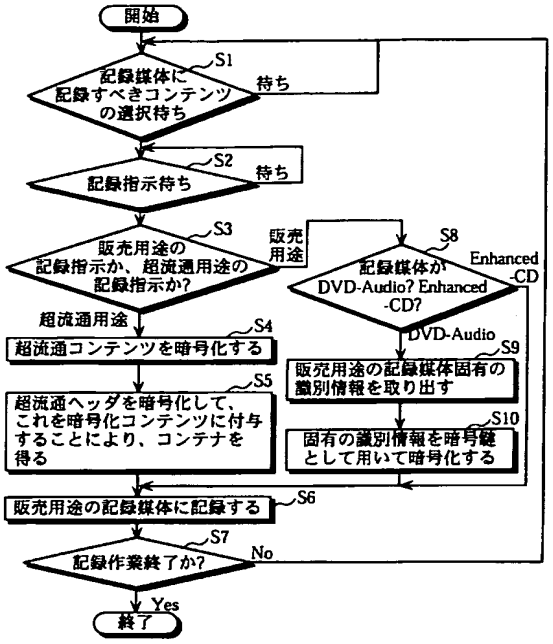
【図６】



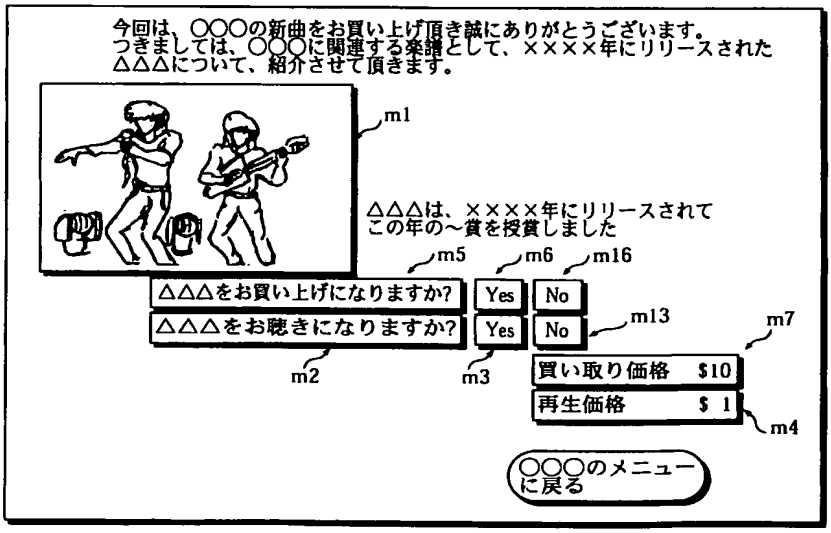
【図７】



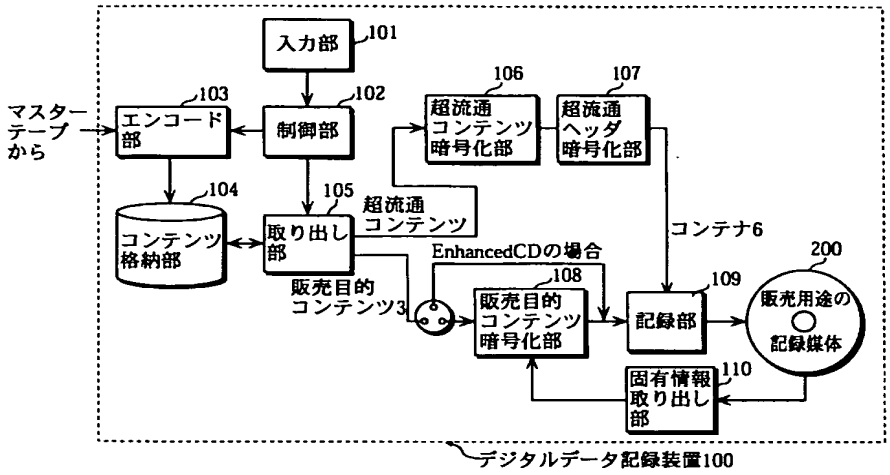
【図１０】



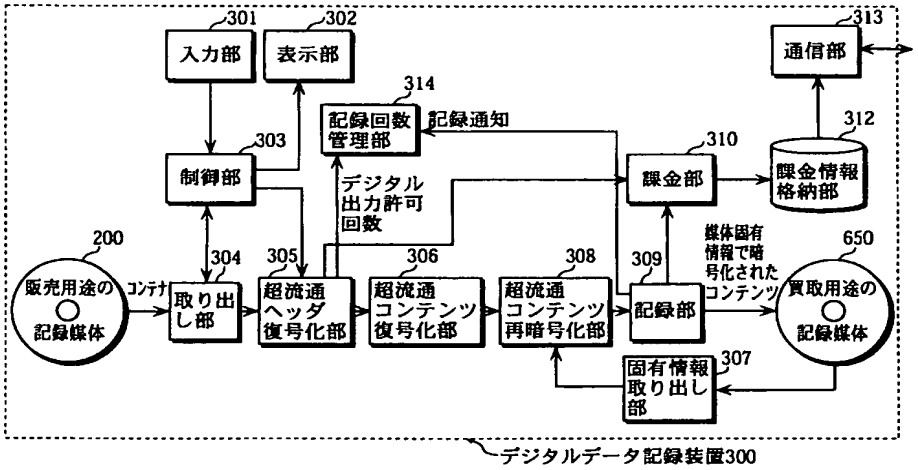
【図８】



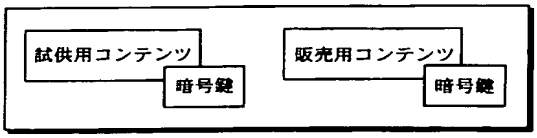
【図９】



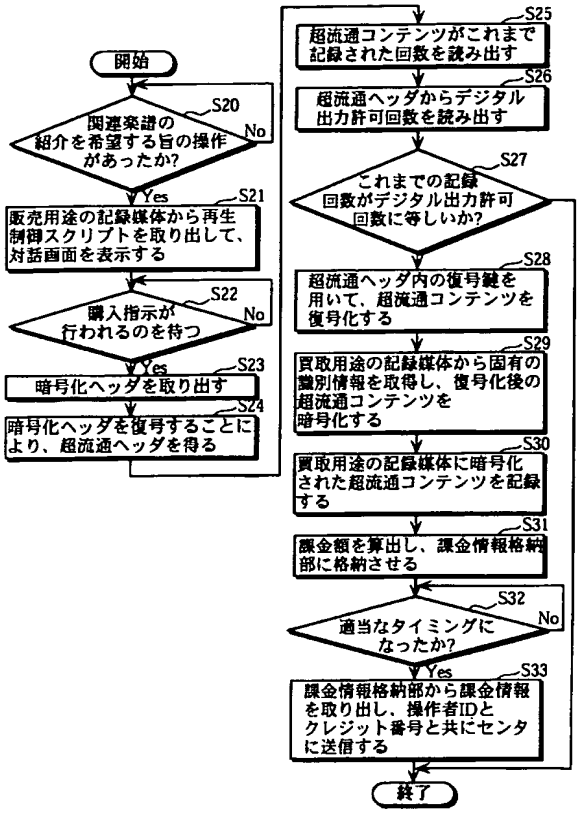
【図１１】



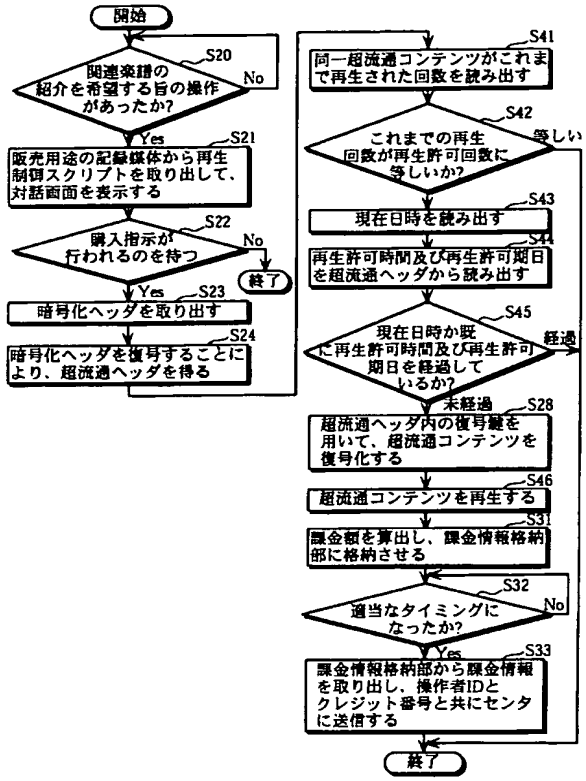
【図２０】



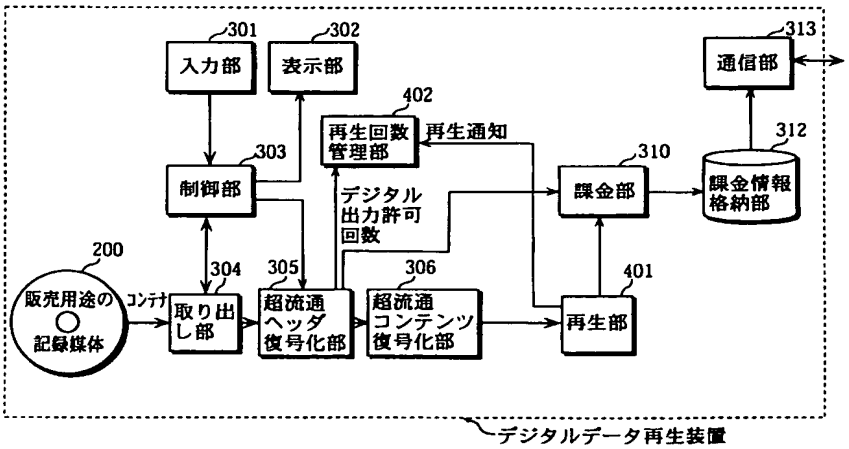
【図１２】



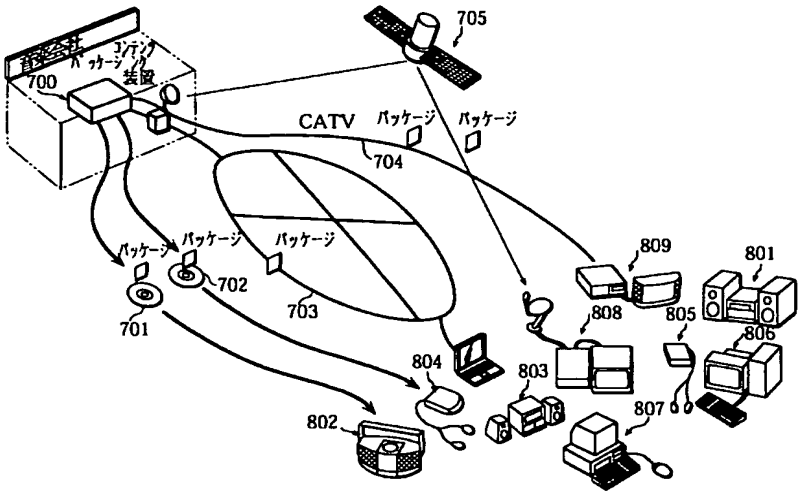
【図１４】



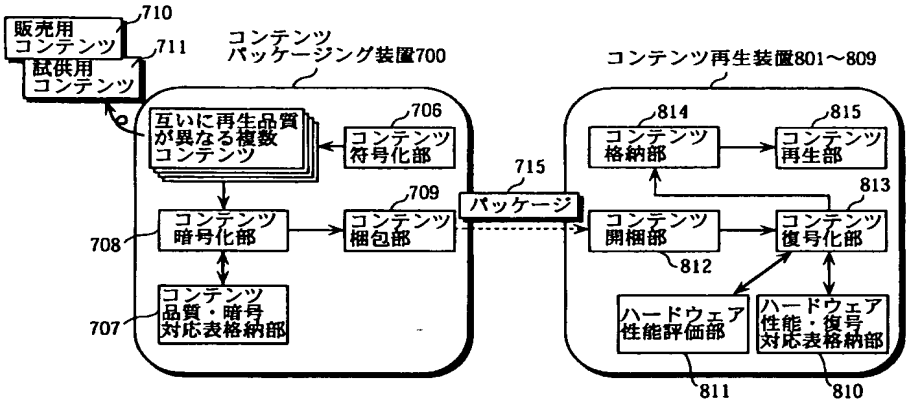
【図１３】



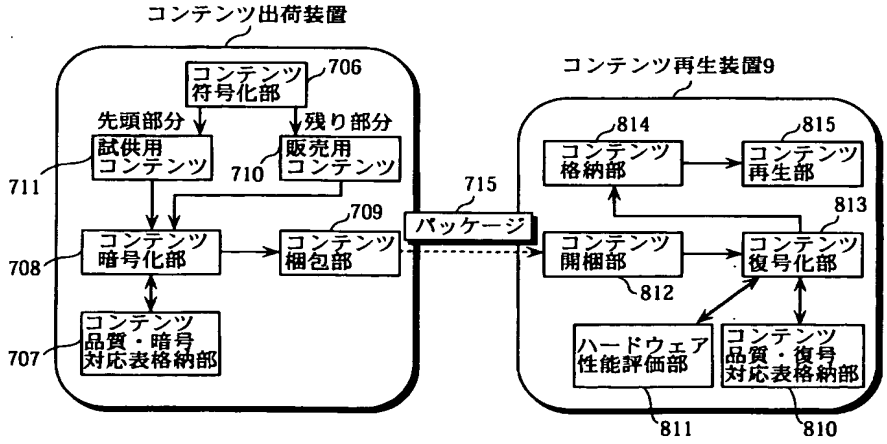
【図１５】



【図１６】



【図１９】



【図１７】

（ａ）

コンテンツレベル	量子化ビット数	サンプリング周波数
ランク1	24 bit	96 KHz
ランク2	16 bit	44.1 KHz
ランク3	16 bit	22.05 KHz

（ｂ）

コンテンツレベル	暗号鍵	暗号アルゴリズム
ランク1	1024 bit	RSA
ランク2	512 bit	RSA
ランク3	56 bit	DES

（ｃ）

ハードウェア性能レベル	復号鍵	復号アルゴリズム
ランクA	1024 bit	RSA
ランクB	512 bit	RSA
ランクC	56 bit	DES

フロントページの続き

(72)発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　青山　昇一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　徳田　克己
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　平田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(54)【発明の名称】　コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケージを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能な記録媒体、記録方法、再生方法、パッケージング方法、コンテンツパッケージング装置と、コンテンツ再生装置とからなるシステム。